

*PEOPLE Light Pack Community Edition*

Progettazione di dettaglio

19 dicembre 2012



---

*PEOPLE Light Pack Community Edition*

## Progetto di dettaglio

Versione 1.0 del 19 dicembre 2012 (PEOPLE LPCE 1.0.doc)

### *Storia delle versioni:*

<i>Versione</i>	<i>Data</i>	<i>A cura di</i>	<i>Note</i>
0.1	13/11/2012	Linea Comune S.p.A.	Documento realizzato in forma di prima bozza.
0.2	19/11/2012	Linea Comune S.p.A.	Aggiornamento prima forma di bozza.
0.3	14/12/2012	Linea Comune S.p.A.	Aggiornamento seconda forma bozza.
1.0	19/12/2012	Linea Comune S.p.A.	Primo rilascio forma finale

## Sommario

---

1. Contesto di riferimento .....	5
1.1. PEOPLE LPCE.....	6
2. Requisiti .....	11
2.1. Requisiti di contesto.....	11
2.2. Requisiti normativi .....	14
2.3. Requisiti di piattaforma.....	17
2.4. Requisiti di integrazione .....	18
2.5. Requisiti di estensione dei servizi .....	19
3. Architettura funzionale .....	22
3.1. Introduzione alla soluzione .....	22
3.2. Servizi infrastrutturali.....	23
3.2.1. Firma digitale.....	24
3.2.2. Verifica firma digitale online .....	24
3.2.3. Verifica marca temporale .....	24
3.2.4. Spazio cittadino/operatore.....	25
3.2.5. Creazione PDF/A .....	26
3.2.6. Validazione formati file.....	26
3.2.7. Riferimento documenti online .....	27
3.2.8. Sistema prenotazioni .....	28
3.3. Gestione identità .....	30
3.3.1. Gestione integrata operatori di back-office .....	31
3.3.2. Gestione integrata dell'identità dei cittadini .....	31
3.3.3. Gestione integrata delle smartcard (CNS, CRS) .....	31
3.4. Pagamenti e incassi.....	32
3.5. Sottomissione istanze .....	32
3.6. Composizione dinamica form .....	33
3.7. Servizi verticali.....	34
3.7.1. IMU .....	34
3.7.2. Cambio di residenza .....	34
3.7.3. Autocertificazioni precompilate .....	34
3.8. Adattabilità della soluzione .....	34

4. Architettura tecnica .....	36
4.1. Stack tecnologico di riferimento .....	38
4.2. Piattaforma .....	38
4.2.1. Gestione dell'identità .....	38
4.2.1.1. Access Manager OpenAM .....	39
4.2.1.2. Memorizzazione profili utente OpenLDAP .....	41
4.2.1.1. Console di Registrazione .....	43
4.2.2. Pagamenti e Incassi.....	43
4.2.3. Plugin integrazione PEOPLE .....	45
4.2.3.1. Plugin modulo CA-People.....	45
4.2.3.2. Plugin modulo Pagamenti e incassi (MIP) .....	46
4.2.4. Profili utente e sicurezza applicativa.....	46
4.2.4.1. Struttura della directory utenti .....	47
• cn=amministratori,dc=sp2con-demo,dc=it .....	47
• cn=cittadini,dc=sp2con-demo,dc=it .....	47
• cn=operatori,dc=sp2con-demo,dc=it .....	47
4.2.4.2. Memmorizzazione profili utente OpenLDAP .....	47
4.2.4.3. Sicurezza applicativa .....	48
4.2.5. Interfacce di front-end (cittadino) .....	48
4.2.6. Banche dati .....	50
5. Trasferimento e manutenzione .....	51
5.1. Codice sorgente .....	51
5.2. Licenza di distribuzione.....	51
5.3. Dispiegamento.....	51
5.4. Formazione del personale .....	52
5.5. Manutenzione correttiva.....	53
Appendice 1: Le possibili soluzioni.....	54
1.1. Modulo gestione e federazione delle identità .....	56
1.2. Modulo contenitore delle identità.....	57
1.3. Funzioni del sistema.....	58
1.4. La piattaforma di sistema .....	59
1.5. La sicurezza.....	60
1.6. Valutazione delle soluzioni individuate.....	61
Appendice 2: Prove sperimentali .....	62
1.1. Configurazioni .....	62
1.2. Modalità di esecuzione delle prove .....	63
1.3. Risultati emersi .....	63
Appendice 3: Quadro normativo .....	66

Allegato A ..... 70

---

## 1. Contesto di riferimento

---

Gli Enti pubblici, nel perseguire obiettivi d'innovazione istituzionale e rafforzamento della governance locale, anche in ottica di attuazione delle politiche di avvicinamento del sistema pubblica amministrazione territoriale al mondo economico, sociale ed ai singoli cittadini, ai fini di rimuovere il carico burocratico che su loro pesa, necessitano di promuovere una soluzione per la realizzazione di processi di modernizzazione della macchina amministrativa. L'obiettivo primario, nell'ambito dei processi di E-Government, è agevolare l'erogazione di servizi e di consultazione informativa a cittadini e professionisti che ne hanno diritto, secondo quanto previsto dalle normative.

Questo contesto rende necessario realizzare un progetto d'innovazione che implica l'adozione di soluzioni tecnologiche adeguate e a supporto delle prassi amministrative. Ne consegue un diretto approccio riorganizzativo oltre che l'adozione di soluzioni applicative finalizzate a permettere agli Enti di gestire l'attività amministrativa in ambiente digitale.

In tale ambito si colloca il progetto PEOPLE<sup>1</sup>, concluso ad ottobre 2006, il quale prevedeva la condivisione delle migliori pratiche nell'erogazione dei servizi pubblici online, tramite la condivisione e la standardizzazione di un modello di community. Ciò ha consentito nel tempo di sviluppare tutta una serie di servizi iscrivibili e fruibili a riuso secondo quanto previsto dalla normativa nazionale in materia (Legge 27 dicembre 2002 n.289, Direttiva del Ministro Innovazione e Tecnologie 19 dicembre 2003, Legge 30 dicembre 2004 n.311 - Finanziaria 2005, DPCM 31 maggio 2005, Direttiva del Ministro Innovazione Tecnologie 4 gennaio 2005).

I servizi sviluppati nel tempo, in via sperimentale, sono più di 200 e rappresentano il 95% del fabbisogno degli Enti Locali. I servizi, suddivisi in comunità di pratica, sono classificati in: edilizia, anagrafe, tributi, mobilità, sviluppo economico, servizi alla persona, pagamenti e scuola.

Tra gli obiettivi del progetto originale si ricordano:

- La standardizzazione dei processi di E-Government
- La diffusione delle nuove tecnologie, al fine di offrire supporto ai piccoli Comuni in modo tale che questi potessero condividere pratiche ed esperienze degli Enti Locali più "grandi" e con maggior capacità d'investimento
- Il trattamento paritario, garantito dall'opportunità, per tutti gli Enti, di poter usufruire degli stessi mezzi
- La possibilità di riutilizzo della piattaforma da parte di tutti gli Enti
- La creazione di un modello organizzativo in *community* (comunità di pratica) per l'utilizzo, lo sviluppo e la standardizzazione dei processi e della modellazione gestiti dalla piattaforma
- La modellazione e la definizione della struttura di messaggi tra front office e back office secondo strutture precostituite
- Lo sviluppo di un modello tecnologico di riferimento per l'interazione front office - back office basato sulla suddivisione: layer front-end, layer back-end

---

<sup>1</sup> Progetto Enti Online Portali Locali E-government

Nelle intenzioni originali, il concetto di *community* era quello di una comunità di pratica che condividesse le specifiche progettuali ad un livello di dettaglio tale da coinvolgere la revisione dei processi amministrativi; tale comunità doveva essere successivamente mantenuta nel tempo. L'esperienza ha dimostrato che si sono rese, invece, necessarie numerose personalizzazioni della piattaforma presso i vari Enti al fine di adattarsi alle diverse declinazioni dell'interpretazione delle norme, dando, di fatto, origine ad una molteplicità di servizi e personalizzazioni del framework di base.

## 1.1. PEOPLE LPCE<sup>2</sup>

L'ideazione di un sistema PEOPLE Light Pack Community Edition (LPCE) nasce con lo scopo di mantenere e far evolvere tutti gli obiettivi, i servizi ed i prodotti realizzati dal precedente progetto PEOPLE, tenendo presente lo stato dell'arte delle tecnologie IT, e confermando la vocazione spinta al mondo Open Source che ha caratterizzato anche il progetto PEOPLE originario.

Facendo tesoro dell'esperienza pregressa, è stato adottato un approccio progettuale di semplificazione strutturale e tecnologica nello scambio d'informazioni tra il front end ed il back office eliminando il vincolo di una modellazione precostituita. Il modello logico sottostante, come verrà dettagliato nel seguito, è modulare (suddivisione per componenti logici) ma fortemente coeso; esso si fonda su due macro aree: i servizi infrastrutturali ed i servizi verticali on line.

La community, stante la precedente esperienza, assume ora un ruolo principale nella condivisione dei processi di erogazione, nell'interpretazione della normativa e della relativa scelta dei dati coinvolti nei processi.

Il presente progetto è frutto di una collaborazione di co-progettazione tra Comune di Firenze e A.N.C.I.<sup>3</sup>, alla quale è affidata la gestione del progetto (Project Management), il coordinamento ed il monitoraggio finalizzato al raggiungimento degli obiettivi. Inoltre A.N.C.I. sovrintende la definizione di regole condivise e la loro introduzione nelle comunità riusanti, a livello nazionale, garantendo lo sviluppo evolutivo della soluzione nel complesso. Lo scopo di questa piattaforma, denominata "PEOPLE *Light Pack Community Edition*", è quello di estendere e semplificare ma non sostituire la precedente, in particolare verrà adottata una progettazione modulare. Vi saranno specifici blocchi logici (moduli) che svolgeranno funzioni infrastrutturali del sistema, sopra i quali dei diversi moduli andranno a realizzare l'erogazione di servizi verticali.

Nell'ambito del presente progetto verranno definite le architetture software, le funzioni svolte dai moduli infrastrutturali e verranno individuati i sistemi, gli applicativi ed i linguaggi, ad oggi allo stato dell'arte, per l'implementazione dei moduli stessi, inoltre verrà realizzata l'implementazione dei moduli stessi. Saranno anche sviluppati tre servizi verticali (IMU, cambio residenza ed autocertificazioni precompilate) sperimentali allo scopo di validare i requisiti e le finalità del progetto (non ultimo verificare la velocità d'implementazione di nuove applicazioni). Tale approccio progettuale preserverà la validità nel

<sup>2</sup> Progetto Enti Online Portali Locali E-government Light Pack Community Edition

<sup>3</sup> Associazione Nazionale Comuni Italiani

tempo dei blocchi logici e permetterà altresì la possibilità di aggiornare via via l'implementazione degli stessi mantenendo la tecnologia allo stato dell'arte.

Come verrà dettagliato nel prosieguo del documento, PEOPLE LPCE rappresenta un'evoluzione nella continuità del progetto PEOPLE, una somma di esperienze che vogliono concretizzarsi nel superamento dei limiti riscontrati e che sono riassunte in due concetti chiave: **Light** e **Community**.

Light in quanto alcune delle funzionalità di PEOPLE possono trarre vantaggio da una riprogettazione in termini di semplificazione tecnologica. Oggi le moderne tecnologie ci indicano che non vi è necessità di realizzare software specifici per:

- generare maschere utente interattive
- articolare la navigazione e interazione utente in una serie di maschere susseguenti
- controllare la valorizzazione delle informazioni sulla base di quelle già inserite

esistono, infatti, framework maturati nel corso degli ultimi anni che automatizzano tutto quanto necessario direttamente negli ambienti di sviluppo. Di fatto si riescono a produrre, codificando in tempi rapidissimi, front office moderni e più flessibili senza necessità di dover sviluppare e mantenere componenti generiche che data la loro natura (appunto "generica") richiedono di sostenere costi che usualmente non collimano con un opportuno valore di ritorno atteso.

Vi è quindi una necessità di recuperare le normali logiche di un'analisi costi / benefici e di concentrare diversamente gli sforzi e le competenze tecnico amministrative per trovare un percorso che possa garantire, con il minor sforzo, un adeguamento in tempi rapidi per:

- creare nuovi servizi predisponendo interfacce standardizzate verso sistemi terzi
- creare nuovi servizi riutilizzando quelli esistenti (operazione possibile solo se rispettato il punto precedente)
- aumentare la fruizione dei servizi online predisponendo per i servizi di front end forme assistenziali al cittadino che migliorino la user experience e che consentano di superare i limiti di comprensione del linguaggio amministrativo
- disporre di un sistema che consenta facilmente di adeguare i servizi al variare della normativa a fronte di un'interpretazione comune e di un'analisi dati e di processo condivisa (massimizzazione delle logiche di riuso e sostenibilità dei servizi di E-Government)
- offrire il medesimo servizio in forme interattive differenti secondo canale di erogazione preservando la medesima fonte dati, logiche di elaborazione dati e di articolazione dei processi
- realizzare e mantenere nuovi servizi con competenze recuperabili facilmente nel mercato ICT, grazie all'utilizzo di tecnologie standard

Affinché quanto elencato possa essere sostenuto nel tempo e divulgato a tutta una moltitudine di Enti PAL (Pubblica Amministrazione Locale), vi è la necessità di preservare quella che originariamente, già presente nel progetto PEOPLE, era "l'idea di Community", aumentandone la centralità. La governance di A.N.C.I. su questo progetto risulta, quindi, determinante per far sì che la

community agisca come un singolo organismo: coordinato, coeso e maggiormente finalizzato all'utilità comune.

Inoltre l'introduzione di prodotti FLOSS<sup>4</sup> assicura flessibilità attraverso aderenza agli standard tecnologici di mercato noti e aperti e prodotti più moderni attraverso il continuo aggiornamento sostenuto da comunità e aziende. Il risultato è che viene reso disponibile un set di base di funzioni più ampio, a beneficio dei processi d'integrazione tra componenti e/o sistemi.

Il nuovo progetto porterà ad una razionalizzazione e riduzione dei costi grazie alla:

- semplificazione nello scambio dei flussi tra front end e back office (dato aggregato in forma flessibile, di volta in volta variabile)
- semplificazione delle interfacce di comunicazione (diversa standardizzazione al posto della modellazione predeterminata)
- flessibilità nell'invocare le funzioni, di volta in volta necessarie, senza necessità di modificare le logiche predeterminate di un framework di base (p.es obbligatorietà invocazione funzioni di workflow per servizi di visura demografica, salva/ripristina per servizi che non articolano procedimenti)
- Interazione con sistemi terzi estendibile e non determinata a priori (invocazione in momenti differenti, secondo necessità del servizio, del sistema pagamenti, firma digitale, etc.)

Si ricorda che, nel precedente progetto, alcune funzioni non necessarie erano sempre articolate nei flussi dati controllati dal framework (ad es. l'utilizzo del workflow per le visure demografiche appariva evidentemente sovrastrutturato) e l'interazione con sistemi terzi era strutturata in modo predeterminato e l'inserimento di ulteriori moduli infrastrutturali richiedeva modifiche al framework di base.

La semplificazione strutturale del nuovo progetto LPCE, unita alla semplificazione nello scambio dei flussi tra front end e back office (dato aggregato in forma flessibile, di volta in volta variabile), porterà una consistente riduzione e razionalizzazione dei costi per lo sviluppo, la manutenzione e la personalizzazione dei servizi stessi.

Revisionando la soluzione del precedente sistema PEOPLE, verranno estesi i servizi infrastrutturali e nel complesso adeguati alle vigenti normative (es. i servizi di firma, di verifica del timbro digitale, cambio di residenza, I.M.U., etc.)

Nel presente progetto, A.N.C.I. è responsabile delle attività di dispiegamento per gli Enti partecipanti e provvederà all'analisi dei diversi contesti di destinazione presenti in ciascuno degli Enti coinvolti. Condividerà il modello generale di erogazione e promuoverà tutta una serie di attività per adattare i sistemi oggi in produzione, predisponendoli secondo lo standard previsto dal PEOPLE LPCE compreso il dispiegamento e integrazione dei servizi della piattaforma, secondo necessità, quali:

- Composizione dinamica e flessibile dei form e dei servizi
- Sottomissione istanze

---

<sup>4</sup> Free/Libre and Open Source Software

- Pagamenti e incassi
- Gestione identità
  - Access manager
  - Profili utente/operatori
  - Console identità
- Servizi infrastrutturali
  - Firma digitale
  - Verifica firma digitale online
  - Verifica marca temporale
  - Spazio cittadino / operatore
  - Creazione PDF/A
  - Validazione formati file
  - Riferimento documenti online
  - Sistema Prenotazioni

Realizzerà infine il dispiegamento ulteriore dei servizi sperimentali verticali precedentemente indicati:

- IMU
- Autocertificazioni precompilate
- Richiesta cambio residenza

Questi servizi sono stati scelti in quanto risultati più di uso comune.

Considerata l'eterogeneità degli Enti possibili utilizzatori del presente progetto (Comuni, Province, ALI<sup>5</sup>, CST<sup>6</sup>, etc.), ognuno dei quali ha una situazione organizzativa diversa, è stata presa come parametro di riferimento la situazione più complessa tratta dall'esperienza diretta del Centro Servizi del Comune di Firenze, in modo tale che tutte le restanti situazioni ricadano in un sottoinsieme della soluzione individuata.

Con questa modalità tutti gli Enti, sulla base di alcune scelte analizzate e intraprese in accordo comune, potranno beneficiare del progetto PEOPLE LPCE sia in forma parziale, sia in forma integrale (ciò sarà reso possibile grazie alla progettazione per moduli autocontenuti e grazie ai nuovi prodotti basati su standard di mercato noti e "aperti").

Tutti gli Enti infine avranno una forma comune (adozione medesimo standard di base) per l'erogazione ed il riuso dei servizi.

Nell'ambito di questa progettualità sarà presentato il modello e rilasciato un documento di linee guida che garantirà autonomia ai singoli Enti partecipanti per evolvere in modo indipendente la soluzione interscambiando i nuovi servizi realizzati.

Particolare attenzione sarà posta alla documentazione, che permetterà agli Enti riusanti, assieme alla disponibilità di codice sorgente, di poter far mantenere o evolvere il sistema LPCE a qualunque fornitore ICT reperibile sul mercato.

---

<sup>5</sup> Alleanza per l'Innovazione

<sup>6</sup> Centro Servizi Territoriale

Nel complesso, parte degli obiettivi è ottenere un maggior efficientamento dei servizi e del riuso, garantendo, per quanto possibile, una razionalizzazione della spesa e un'evoluzione efficace delle funzioni.

## 2. Requisiti

---

### 2.1. Requisiti di contesto

Molti sono i fattori che contribuiscono alla necessità di aggiornare la soluzione PEOPLE, pur preservando gli investimenti della soluzione precedente; di seguito si richiamano brevemente i principali.

#### **Contenimento dei costi**

Il contenimento dei costi è, per le pubbliche amministrazioni, una priorità; pertanto questo progetto avrà l'obiettivo fondamentale di ottimizzare la piattaforma in modo da ridurre tanto i costi sia nelle fasi evolutive quanto nelle fasi ricorrenti degli ambienti di servizio

#### **Condivisione delle risorse tra Enti**

Dovrà essere possibile poter condividere tra Enti componenti software e componenti tecnologiche infrastrutturali.

#### **Utilizzo di software FLOSS basati su standard noti e aperti di mercato**

La piattaforma utilizzerà software FLOSS e basati su standard di mercato interoperabili.

Tale scelta permetterà la possibilità di disporre di un "parco fornitori" molto più ampio, oltre che la possibilità di poter modificare interi blocchi funzionali o componenti del progetto in caso di bisogno senza i vincoli dettati da soluzioni monolitiche dei vendor. Infatti la strutturazione dei servizi, numerosi e di varia complessità, beneficerà dalla scelta di soluzioni "open" dato che vengono meno molti vincoli delle soluzioni proprietarie e contestualmente aumenta il numero dei componenti interoperabili e riutilizzabili.

Verranno utilizzati componenti infrastrutturali "as-is" incluse le funzioni "native di integrazione" che consentono il colloquio nell'ambito della soluzione secondo standard noti (nessuna procedura realizzata ad-hoc)

#### **Multipiattaforma**

La soluzione dovrà assicurare flessibilità di funzionamento su un predeterminato numero di ambienti operativi e, una volta assicurata l'aderenza delle interfacce agli standard, potrà integrarsi con componenti implementate su stack tecnologici differenti.

#### **Multicanalità**

I servizi di oggi hanno necessità di essere erogati in ambiente multicanale. La soluzione promuoverà le logiche di erogazione dei servizi non limitando la fruizione del servizio al canale web, ma tenendo conto, nelle fasi di progettazione, anche dei moderni canali di interazione come piattaforme mobili smartphone e tablet e dei canali di social media networking.

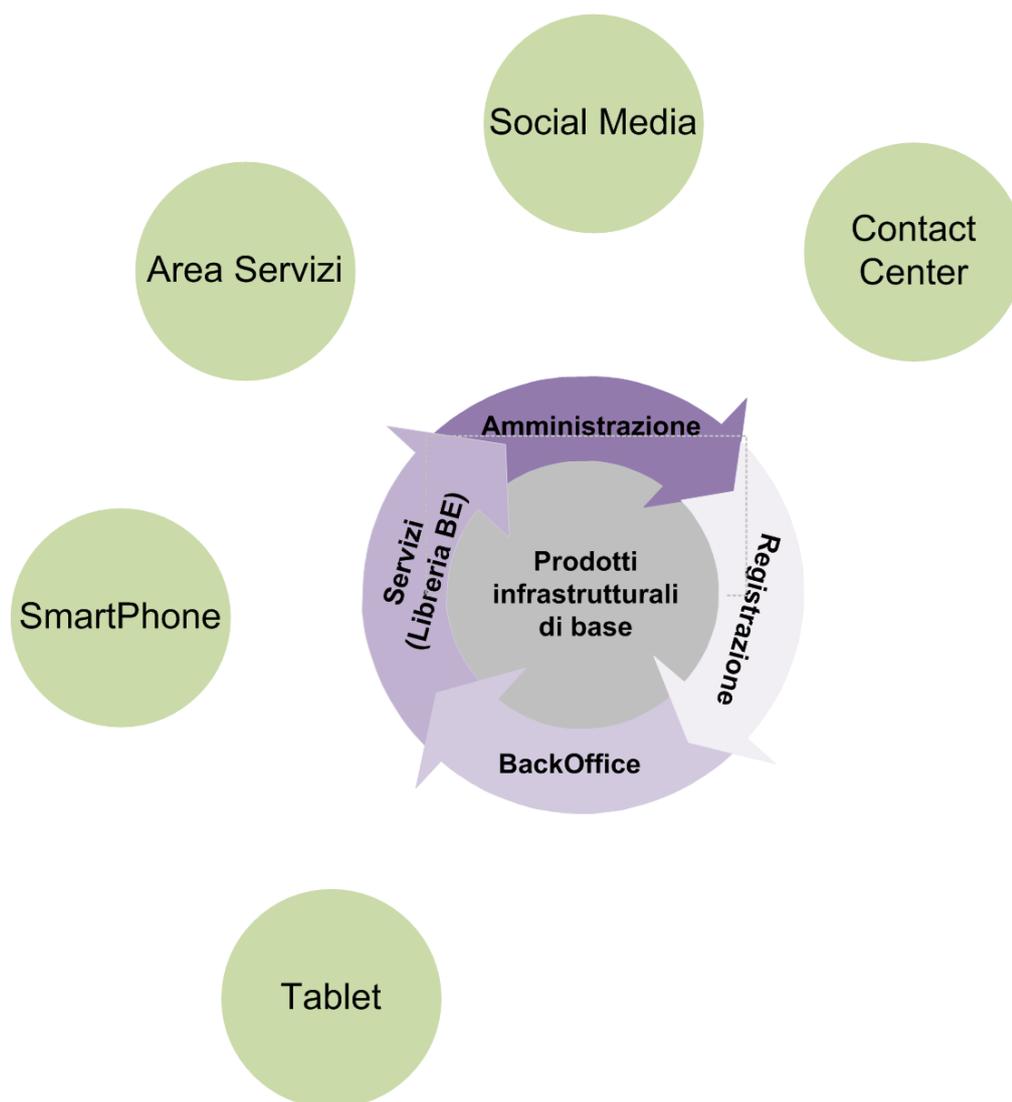


Figura 1

### **Dati aggregabili in richieste/risposte secondo necessità**

Nel caso di una modellazione “determinata a priori” si rende necessaria una duplicazione d’uso della tecnologia: una per la strutturazione dei contenuti (fissa) ed un’altra per la standardizzazione delle interfacce. Questa modellazione costituisce un vincolo e determina un eccesso nella strutturazione di tutta una serie di informazioni a cui farà seguito un’impossibilità di valorizzazione o una valorizzazione marginale rispetto a quanto prestabilito. Inoltre obbliga, in ogni caso, l’implementazione a gestire “il tutto”, comprese le parti di dato strutturato ma non valorizzato. Stante l’esperienza che rivela che l’interscambio con il back-office richiede un insieme di dati molto ridotto, la semplificazione adottata nella soluzione PEOPLE LPCE migliora lo standard che definisce, attraverso l’uso di un’unica tecnologia, la descrizione dell’interfaccia e il “contenuto informativo” dei dati, non le singole richieste/risposte e produce una traducibilità delle strutture dati con diversi formalismi XML, JSON, RDF (predisposizione multicanalità e diversità tecnologica dei layer back end e di front end). I dati risulteranno aggregabili (flessibilità del modello) in richieste/risposte secondo necessità. Ne conseguono sviluppi e adattamenti più rapidi, basati esclusivamente sul dato valorizzato e una diretta ottimizzazione dei costi.

## Ergonomia

I nuovi servizi assicureranno a ciascun Ente la possibilità di migliorare l'interazione utente e la possibilità di offrire la stessa "user experience" derivata da PEOPLE oppure di poterne adottare una nuova.

Con l'adozione dei moderni strati tecnologici "rich-component" (ad esempio Vaadin) è assicurata una molteplicità di controlli per una costruzione visuale (tramite l'utilizzo degli ambienti di sviluppo) delle interfacce utente. Non vi sarà più la necessità di dover riscrivere logiche e implementazioni per la generazione del controllo stesso. L'Ente potrà quindi meglio curare gli aspetti funzionali per assicurare:

- una valorizzazione assistita e più informata per l'utente finale
- la medesima interazione e disposizione dei controlli offerta dal canale di base
- il continuum grafico per l'immagine coordinata

Inoltre questo tipo di tecnologia mette a disposizione funzionalità per descrivere (in modo dichiarativo) il susseguirsi della navigazione tra le diverse maschere utente.

Un ulteriore beneficio sarà dato dalla possibilità di utilizzare un minor numero di righe di codice dedicate al controllo delle informazioni immesse e agli stati di dipendenza tra le valorizzazioni dei controlli tra maschere precedenti e successive; ad esempio sarà ora più semplice realizzare i controlli sui dati immessi in form suddivisi in più pagine.

Sarà, inoltre, resa molto più agevole la possibilità di modificare l'iter di un processo potendo introdurre, in un qualunque punto, l'interazione con moduli e/o sistemi terzi (p.es. identità, firma digitale, verifica formato file, creazione pdf/a, etc.).

I servizi (layer di front-end) basati su questo tipo di tecnologia potranno essere dispiegati in ambienti standalone ma anche opzionalmente integrati in altri ambienti come ad esempio quelli di portale affinché coesistano, a tendere, nella medesima interfaccia, contenuti informativi, multimediali e servizi dispositivi (user integration).

## Riuso

Il progetto realizzato dovrà possedere le caratteristiche per poter essere eventualmente inserito nel catalogo nazionale del riuso; ovvero dovrà soddisfare i seguenti requisiti<sup>7</sup> che stabiliscono che un oggetto sarà tanto più facilmente riusabile se:

- possiede un insieme di caratteristiche tecniche di base, prima tra tutte l'interoperabilità e la cooperazione, che ne permettono l'adattamento a vari contesti, in tempi e costi contenuti
- il riuso è riferito ai singoli componenti (granularità dell'Oggetto) anziché ad intere applicazioni (Oggetto monolitico di tipo verticale)
- è maggiore il numero di amministrazioni pubbliche che fanno riferimento agli stessi domini funzionali

---

<sup>7</sup> Cfr. "Check List per valutazione idoneità riuso" CNIPA

- è maggiore la “qualità” dell’oggetto candidato: soggetto o meno a licenza; composto completamente da componenti open o meno; etc.
- è corredato da una documentazione progettuale, completa e prodotta con notazioni standard, tale che soggetti diversi da quelli che lo hanno originariamente realizzato possano facilmente modificarlo e adattarlo
- è corredato da una documentazione d’uso costruita in modo da poter essere anch’essa modificata e adattata con facilità ad altri contesti
- è corredato da una adeguata ed esaustiva documentazione sui test a cui l’Oggetto stesso deve essere sottoposto ai fini del riuso in altri contesti ed è corredato di casi di test riusabili

## 2.2. Requisiti normativi

Il presente documento è stato sviluppato nello spirito di seguire le norme di seguito riportate, Dovrà, in ogni caso, essere cura delle stazioni appaltanti per i singoli servizi specificare quali normative dovranno essere rispettate oltreché aggiornare i requisiti a seguito dell’evoluzione normativa ed in conformità delle specifiche norme dell’Ente.

Essendo la modularità e la flessibilità delle specifiche fondanti il progetto PEOPLE LPCE, viene lasciato lo spazio necessario per l’implementazione di eventuali interpretazioni normative da parte dei singoli Enti.

### **Imposta Municipale Propria (IMU)**

Tra le novità contenute nella manovra c.d. “Salva Italia”, recata dal D.L. 6 dicembre 2011, n. 201 (Decreto Monti), convertito, con modificazioni, dalla Legge 22 dicembre 2011, n. 214, recante “Disposizioni urgenti per la crescita, l’equità e il consolidamento dei conti pubblici”, in vigore dal 6 dicembre 2011, vi è la rimodulazione del prelievo sugli immobili attraverso l’abolizione dell’ICI e l’introduzione dell’imposta municipale propria (IMU), che sostituisce l’ICI ed anche la tassazione del reddito fondiario degli immobili non locati.

Come prevede espressamente il primo comma dell’art.13 del Decreto Monti, l’IMU è applicata in tutti i Comuni del territorio nazionale, inclusi, anche i Comuni situati nei territori delle Regioni a statuto speciale e delle Province autonome.

### **Cambio di residenza**

Per quanto riguarda i trasferimenti di residenza da altro Comune o dall'estero, i cambi di abitazione all'interno del Comune e le cancellazioni per emigrazione all'estero, dal 9 maggio sono entrate in vigore le nuove norme anagrafiche relative ai "cambi di abitazione in tempo reale". Il Decreto Legge 9 febbraio 2012, n.5, convertito in Legge 4 aprile 2012, n. 35, introduce nuove disposizioni in materia anagrafica, riguardanti le modalità con le quali effettuare le dichiarazioni anagrafiche di cui all'art. 13, comma 1, lett. a), b) e c) del Decreto del Presidente della Repubblica 30 maggio 1989, n. 223, ossia:

- per l’iscrizione anagrafica con provenienza da altro Comune
- per l’iscrizione anagrafica con provenienza dall’estero
- per il cambio di abitazione all’interno del Comune
- per l’emigrazione all’estero

A decorrere dal 9 maggio 2012 i cittadini potranno presentare le dichiarazioni anagrafiche utilizzando i nuovi moduli appositamente predisposti dal Ministero

dell'Interno, debitamente compilati e sottoscritti e corredati della documentazione indicata dal Ministero stesso

### **Accessibilità**

La Legge n. 4 del 9 gennaio 2004, comunemente nota come "Legge Stanca", prendendo spunto dal dettato costituzionale che stabilisce il principio di uguaglianza, ha l'obiettivo di abbattere le "barriere virtuali" che limitano l'accesso dei disabili alla società dell'informazione e li escludono dal mondo del lavoro.

Questa Legge stabilisce che i le Pubbliche Amministrazioni debbano realizzare siti accessibili a tutti. È previsto, infatti, che i nuovi contratti stipulati dalla PA per la realizzazione di siti Internet siano colpiti da nullità, qualora non rispettino i requisiti di accessibilità, comportando responsabilità di carattere dirigenziale e disciplinare.

Tramite il regolamento governativo (DPR 1 marzo 2005, n. 75) sono state fissate le regole generali per la disciplina delle situazioni giuridiche e con il Decreto ministeriale attuativo (DM 8 luglio 2005) sono state stabilite le metodologie tecniche per la verifica dell'accessibilità dei siti Web Content Accessibility Guidelines (WCAG) 1.0.

Tuttavia, lo standard WCAG è in continua evoluzione e l'11 dicembre 2008 è stato pubblicato il nuovo standard del W3C sull'accessibilità dei siti web: le Web Content Accessibility Guidelines (WCAG) 2.0. Ulteriori aggiornamenti sono ancora in corso. In base all'aggiornamento del 26 Aprile 2010 del DM 8 luglio 2005, è possibile affermare che le pagine della PA non devono funzionare, rispetto al requisito n.15 allo standard precedente, dichiarato, necessariamente con "javascript" disabilitato.

E' evidente che l'uso di javascript è fondamentale nell'ammodernamento dei siti web teso ad estendere l'usabilità come prevedono i principi del web 2.0.

Al giorno d'oggi è consuetudine vedere validate tutta una serie di informazioni compilabili in una maschera (form) con interazione per la verifica immediata e realizzata campo per campo, eseguita lato utente (lato client), prima dell'invio della form valorizzata in modo completo.

E' molto frequente che al giorno d'oggi venga utilizzata, tanto per nominarne una, la tecnologia AJAX.

Nello stesso aggiornamento legislativo si trovano anche indicazioni del fatto che in WCAG 2.0, al contrario della v.1.0, non solo la tecnologia javascript è ammessa ma anche, per alcuni aspetti, consigliata per risolvere meglio alcune problematiche relative alla stessa accessibilità.

Deve essere chiaro che "accessibile" non dovrà essere il singolo che servizio (il servizio visto come applicazione software puntuale) ma l'intera struttura del sito finale (p.es. rete civica) nel suo complesso.

Inoltre l'accessibilità non deve essere più pensata per il solo canale web ma va tenuto presente che ci sono metodi e modi per aumentarla tramite diversi dispositivi e ulteriori canali come ad esempio touch screen e ausili audio.

Si evidenzia che la conformità ai criteri di accessibilità non è l'unico fattore che deve essere tenuto presente nella creazione della presentazione per i servizi e per le informazioni, ma ci sono una serie di ulteriori fattori correlati di cui dover tener conto:

1. Sicurezza applicativa
2. Uso di componenti adattative (rich component) per la realizzazione di front end

3. Semplicità manutenzione del software (minor numero di righe di codice)
4. Evoluzione della presentazione del sito nel tempo (p.es. immagine coordinata)
5. Utilizzo medesima tecnologia per la realizzazione delle interfacce verso i back-office
6. Maturità della tecnologia (in numero di anni)
7. Livello di conoscenze tecniche necessarie
8. Trasversalità della tecnologia su altri prodotti
9. Adattabilità ai dispositivi mobili (p.es. smartphone, tablet)

Nel prosieguo del documento verrà resa nota la matrice di compatibilità della tecnologia utilizzata per la realizzazione degli strati di presentazione rispetto alla normativa e agli standard anticipati.

### **Privacy**

La regolamentazione in materia di privacy è definita dal Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” (c.d. Codice della Privacy), in vigore dal 1 gennaio 2004 che, in materia informatica, prevede il rispetto di misure minime di sicurezza ed introduce specifici adempimenti.

Particolare attenzione deve essere posta al c.d. “diritto all’oblio”. Il Garante ha indicato che “nelle ipotesi in cui specifiche disposizioni di settore individuino determinati periodi di tempo per la pubblicazione di atti e provvedimenti amministrativi (es., art. 124, d.lg. n. 267/2000 riguardante le deliberazioni del Comune e della Provincia che devono essere affisse all’albo pretorio, nella sede dell’Ente, per quindici giorni consecutivi), i soggetti pubblici sono tenuti ad assicurare il rispetto dei limiti temporali previsti, rendendoli accessibili sul proprio sito web durante il circoscritto ambito temporale individuato dalle disposizioni normative di riferimento, anche per garantire il diritto all’oblio degli interessati” e che “Trascorsi i predetti periodi di tempo specificatamente individuati, determinate notizie, documenti o sezioni del sito devono essere rimossi dal web o privati degli elementi identificativi degli interessati” (cfr. par. 5.2, richiamato dal par. 6.B del Provvedimento del 2 marzo 2011 recante le “Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web”, pubblicato in G. U. n. 64 del 19 marzo 2011).

In riferimento alla possibilità offerta dal presente progetto di poter far erogare i servizi online anche ad Enti terzi (Centri Servizi, ALI, etc.), si evidenzia che, in tale fattispecie, i servizi erogati non dovranno sostituire funzionalità proprie, per normativa, dell’Ente stesso. Ad esempio i servizi online non dovranno essere soggetti alla normativa per la conservazione sostitutiva, ovvero gestiranno solo un dato temporaneo ai fini di erogazione del servizio e la notifica e la creazione dei documenti saranno riservate sempre alle funzioni di back office.

L’elevata vivacità dell’evoluzione delle norme che governano il settore dell’E-Government, dimostrata negli ultimi anni, richiede che il sistema PEOPLE LPCE

possieda una spiccata flessibilità nell'adattarsi a esigenze e specifiche sempre nuove. Il sistema migliore per garantire una tale flessibilità è l'adozione di un'architettura modulare.

### 2.3. Requisiti di piattaforma

Al fine di garantire alcuni requisiti fondamentali nell'erogazione dei servizi online, la soluzione proposta necessita inevitabilmente di avere alcuni prerequisiti:

1. strutture hardware
2. un ambiente virtualizzato
3. un ambiente di rete inclusi gli apparati periferici e le dovute configurazioni di sicurezza

Chiaramente nessuno dei prerequisiti citati può essere garantito nell'ambito del rilascio della presente soluzione poiché ogni prerequisito elencato può variare in modo sostanziale e differente secondo esigenze, complessità e possibilità d'investimento nei diversi contesti di destinazione.

Per agevolare i rilasci per le successive fasi di dispiegamento e di collaudo, la soluzione sarà consegnata in forma di "macchine virtuali" che costituiranno ambiente dimostrativo autocontenuto. ANCI provvederà all'analisi dei diversi contesti di destinazione e, in collaborazione con ogni Ente, agli adeguamenti necessari per l'estensione degli ambienti di esercizio.

La piattaforma del sistema dovrà garantire l'erogazione dei servizi H24 7/7. Tale requisito è di fondamentale importanza sia per garantire un elevato standard qualitativo, sia per requisiti normativi (ad es. un fermo dell'albo pretorio potrebbe portare all'invalidazione degli atti ivi pubblicati, con illecito amministrativo).

Tale requisito implica che vengano utilizzate architetture di sistema in grado di garantire alta affidabilità e disponibilità.

Dovrà, inoltre, essere prevista un'allocazione flessibile delle risorse di sistema in grado di garantire sempre la necessaria potenza di calcolo alle risorse, anche durante i carichi critici di elaborazione.

I server e gli applicativi di sistema dovranno essere forniti aggiornati e tenuti allineati alle ultime patches rilasciate dal gestore della distribuzione del sistema operativo adottato. Il sistema ed i server utilizzati dovranno essere scelti secondo il criterio della disponibilità in licenza GPL<sup>8</sup>.

In caso di erogazione di servizi in modalità multiente (p.es. Centri Servizi o ALI), data la sensibilità dei dati trattati, le banche dati dovranno essere implementate con opportuna separazione e differenziazione del dato comune base da quello specifico e compartimentato per l'erogazione dei servizi.

La medesima attenzione andrà riservata nella gestione delle configurazioni degli application server. Occorreranno più istanze, per i diversi casi di fault applicativi. In caso di fault di una delle componenti dell'architettura, l'impatto dovrà essere ridotto ad un gruppo di componenti ristretto, partizionando le

---

<sup>8</sup> GNU General Public License

principali componenti, senza inficiare il funzionamento generale del sistema. Il sistema dovrà, quindi, essere progettato per espletare le proprie funzioni anche in modo parziale massimizzando (per quanto fattibile) le possibilità di erogazione del servizio online.

Rimane principio fondamentale che i servizi debbano poter essere dispiegati con il minimo essenziale dei prerequisiti di sistema: tipicamente un webserver e un application server.

## 2.4. Requisiti di integrazione

Dovrà essere possibile realizzare un'architettura modulare completamente integrata, sia a livello locale che remoto.

In particolare, l'integrazione locale dovrà assicurare:

- la costruzione di servizi a partire da quelli già esistenti
- La standardizzazione delle comunicazioni nel servizio tra il nodo di front-end (presentazione informazione e parte interattiva utente) e il nodo di back-end (scambio messaggi con il back office) in modo da garantire la portabilità dei servizi attraverso dispiegamenti diversi.
- La comunicazione intermodulo tramite interfacce basate su standard industriali di mercato.
- Integrazione "nativa" (senza ricorrere a procedure realizzate ad-hoc) tra i prodotti FLOSS selezionati
- La messa a disposizione di adattamenti/plugin tra piattaforma precedente e la nuova componente di gestione dell'identità per assicurare possibilità di coesistenza tra le soluzioni

La componente di identità dovrà funzionare in modalità:

- standalone senza integrazione alcuna
- come SSO (Single Sign On) locale
- predisposta per la federazione e i sistemi di social networking tramite utilizzo di standard industriali di mercato come SAML 2.x, OpenID, OAuth

Il modulo incassi e pagamenti doterà la piattaforma di un'interfaccia di payment gateway strutturata a "plugin" in grado di interagire con sistemi di pagamento di terze parti. Ogni plugin realizza, sulla base di software creato ad-hoc, gli scambi dei flussi informativi con il rispettivo circuito bancario. La molteplicità degli stessi determinerà la capacità del sistema di interfacciarsi con i diversi circuiti bancari presenti sul mercato. Nell'ambito della soluzione saranno rilasciati a riuso i plugin per il colloquio con i seguenti circuiti bancari di pagamento:

- CartaSi
- Unicredit
- Intesa San Paolo

L'integrazione con i sistemi di back office deve essere risolta tenendo conto di due aspetti: uno di lettura dei dati, l'altro di invio o presentazione di istanza. Si hanno per ogni aspetto citato, requisiti diversi. In lettura, l'integrazione è relativamente facile grazie agli standard industriali soap/xml rest/xml, json.

La sottomissione di istanze e/o richieste è un processo complesso le cui caratteristiche possono dipendere dal tipo di richiesta o di istanza. Creare standardizzazione di messaggi con back office diversi non è un obiettivo se non al fine di facilitare la definizione e la realizzazione dei servizi online. La soluzione non offrirà un modello complessivo che riguardi l'insieme di tutti i dati di un particolare settore applicativo (p.es. demografici) ma una modellazione essenziale e specifica sui singoli servizi necessari. Compito della piattaforma è realizzare le componenti standard che possono facilitare la creazione di servizi in questo senso. L'integrazione verso il back office deve essere risolta utilizzando queste componenti standard. Un aspetto ineliminabile è la struttura del contenuto dei messaggi, per risolvere il "colloquio" con i diversi back office a partire dal nodo di back end, è necessario quasi sempre un intervento dei rispettivi fornitori sulla base delle specificità dei back office adottati dall'Ente, quasi mai è possibile un'integrazione basata su standard industriali o noti di mercato.

La struttura applicativa deve essere in grado, con adattamenti alle configurazioni, di utilizzare anche dati come da esempio Oracle, MySQL, etc.

L'utilizzo di prodotti software FLOSS di mercato garantirà l'integrabilità tra le varie componenti (nel rispetto delle matrici di compatibilità). L'adozione di una architettura modulare, oltre a rendere possibile l'integrazione di componenti diverse, garantirà la possibilità di sostituire e/o far evolvere nel tempo specifici moduli, superando così i vincoli imposti dai framework e dalle architetture monolitiche.

Siccome vi è necessità di offrire un'ampia gamma di servizi, la presente soluzione progettuale non si prefigge di coprire la totalità delle esigenze, anche in relazione ai requisiti di multicanalità (vedasi sopra) e di interazione con il cittadino in ambiti più complessi tipicamente gestiti da Comuni maggiori e/o da Centri Servizi (o ALI); tuttavia si rende noto che la piattaforma complessiva deve potersi integrare, nei diversi contesti di destinazione, con ambienti di CMS (Content Management System) e/o di portale e con sistemi di reportistica.

## 2.5. Requisiti di estensione dei servizi

Si basa sull'ipotesi che la maggior parte dei servizi di E-Government possono essere ricondotti a una struttura più generale:

- una compilazione assistita (include le forme di precompilazione e verifiche incrementalì di consistenza nella valorizzazione dati)
- una compilazione strutturata in più passi, alcuni opzionali
- interazione con i back office degli Enti

In alternativa ci sono dei servizi di E-Government che in linea di principio non corrispondono a un procedimento, ad esempio i sistemi di pubblicazione documentale e di gestione delle prenotazioni. Per questo motivo possono essere convenientemente implementati in modalità frontoffice - backoffice. In questi casi non risulta infatti utile una separazione dei due livelli (front-end e

back-end). Usualmente questo caso ricorre qualora vi sia un prodotto di mercato “open” da dover integrare nella piattaforma PEOPLE LPCE.

Si identificano, quindi, due possibili modalità di estensione dei servizi:

- S.1. Per i servizi affini ai procedimenti l'estensione avviene tramite la creazione guidata di maschere e/o tramite scrittura di codice.
- S.2. Per i servizi che differiscono dai procedimenti tramite integrazione di un prodotto di mercato “open” è necessario comunque che il prodotto stesso rispetti una serie di prerequisiti.

Nel primo caso (S.1.), in generale, la fase di compilazione è finalizzata a funzioni di: visura, prenotazioni e presentazione di richieste di istanza alla quale può essere associato un pagamento.

Questa struttura può avere:

- S.1.a. delle comunanze (un “pattern” ricorrente per i servizi di E-Gov). Per questi casi si può realizzare un sistema che permetta di definire moduli online per i servizi a minore complessità in termini di un processo complessivo di compilazione e di interazione con i sistemi terzi (back office, altre componenti funzionali) e tramite un sistema che non richieda la realizzazione di software ad hoc. Pertanto, nella presente fattispecie di servizio, è opportuno l'utilizzo di uno strumento che permetta l'estensione in modo semplice senza programmazione o con una programmazione minimale.
- S.1.b. delle differenze. Quest'ultime non riguardano i backoffice o la compilazione dell'istanza ma la complessità dell'organizzazione del percorso con il quale i passi si susseguono e la necessità di interazione con sistemi terzi diversi. I servizi a maggior complessità devono essere costruiti mantenendo la logica di standardizzazione PEOPLE front office - back office, integrazione sincrona online (tipicamente lettura dati). I servizi di front office, a loro volta, manterranno la loro costruzione secondo logica di disaccoppiamento front end - back end. La parte di front assicurerà le funzioni di interazione utente (cittadino / operatore). La parte di back end assicurerà le logiche di elaborazione e di integrazione con gli specifici sistemi di back office dell'Ente e/o di utilizzo di eventuali strutture dati di disaccoppiamento.

Inoltre vi può essere la necessità di avere controlli su dati locali (p.es. recupero informazione data corrente), controlli incrociati sui campi, branching (inteso come parti condizionali per la prosecuzione del percorso stesso), integrazione con il backoffice per la compilazione in forma assistita o per le verifiche necessarie.

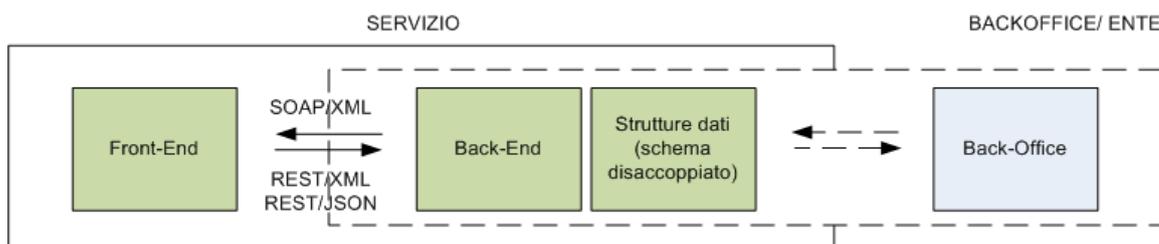


Figura 2

Nel secondo caso (S.2.), i servizi devono poter essere costruiti per realizzare solo il software essenziale che utilizzi il più possibile le componenti standard della piattaforma per le funzioni specifiche realizzate; i servizi dovranno rispettare i seguenti prerequisiti:

- integrarsi con la gestione dell'identità
- integrarsi con i sistemi di pagamento
- essere dotati di Key Performance Indicators per la reportistica
- offrire interfacce API verso sistemi terzi
- utilizzare standard industriali di mercato

Il sistema deve garantire la compatibilità (traducibilità) delle strutture dati con diversi formalismi: SOAP/XML, REST/XML, REST/JSON, RDF. I dati devono essere aggregabili in richieste/risposte secondo necessità.

Tendenzialmente per la migrazione dei servizi esistenti (non inclusa nella presente progettualità), già realizzati nell'ambito del progetto PEOPLE si consiglia di mantenere la compatibilità con quanto esistente (laddove documentato) e riusare le componenti di back end nella loro forma originale per preservare il "colloquio" e gli adattamenti implementati con i sistemi di back office. E' intenzione preservare e non rendere necessario alcun ulteriore adattamento presso le strutture degli Enti.

L'accesso ai dati del back office (propedeutico alla fase successiva di pubblicazione) deve essere garantito sia verso sistemi locali sia verso sistemi remoti di Enti (p.es. caso complesso Centri Servizi o ALI).

Lo schema dati XML interscambiato tra le applicazioni dovrà essere disaccoppiato/ridotto rispetto allo schema dati reale di back office (limitato al dato necessario per l'espletamento del servizio).

Potranno essere supportati servizi creati con linguaggi e per middleware differenti se le interfacce A2A (Application to Application) monteranno la standardizzazione e saranno tecnologicamente abilitate agli standard SOAP/XML, REST/XML e REST/JSON.

Ogni servizio, a prescindere dalla sua tipologia, ad accesso in forma controllata e non anonima è tenuto ad integrarsi con la componente Access Manager (Single Sign On) e deve essere in grado di recuperare:

- l'identità del profilo ed eventuali appartenenze a gruppi
- i dati di autorizzazione applicazioni/funzionalità applicative

Ogni servizio rispetterà la produzione di dati nelle forme indicate (documento di Linee Guida che sarà sviluppato successivamente nell'ambito del progetto) per consentire la valorizzazione dei parametri inerenti gli indicatori chiave di prestazione finalizzati alla successiva produzione di report e statistiche di erogazione/fruizione dei servizi. La soluzione proposta, in tal senso, fornirà indirizzo di predisposizione ma non includerà alcun sistema di reportistica.

## 3. Architettura funzionale

---

Nei paragrafi seguenti verranno descritti i componenti che costituiscono i macroblocchi della piattaforma PEOPLE LPCE.

### 3.1. Introduzione alla soluzione

L'architettura del sistema è costituita da un core di servizi:

- Gestione identità
- Pagamenti e incassi
- Sottomissione istanze
- Composizione dinamica form
- Servizi infrastrutturali

In particolare i servizi infrastrutturali consistono in:

- Firma digitale
- Verifica firma digitale online
- Verifica marca temporale
- Spazio cittadino / operatore
- Creazione PDF/A
- Validazione formati file
- Riferimento documenti online
- Sistema prenotazioni

I quali vanno a realizzare le funzioni base del sistema e permettono di creare delle sovrastrutture di più alto livello che possono, anche grazie alla standardizzazione delle interfacce dati, essere svincolate dagli specifici interfacciamenti e customizzazioni dei singoli Enti.

Il livello di maturità della piattaforma oggetto di realizzazione sarà idoneo per l'erogazione dei servizi di core; a titolo esemplificativo e non esaustivo verranno inoltre realizzati tre servizi verticali:

- IMU
- Cambio di residenza
- Autocertificazioni precompilate

La scelta è ricaduta su tali servizi in quanto di uso più comune e richiesti dagli Enti stessi.

Grazie alla modularità, ad ogni livello, dell'architettura, tali servizi potranno essere erogati tramite diversi front end (web, telefonico, mobile, etc.) Si riporta, in Figura 3, lo schema logico dei componenti di sistema.

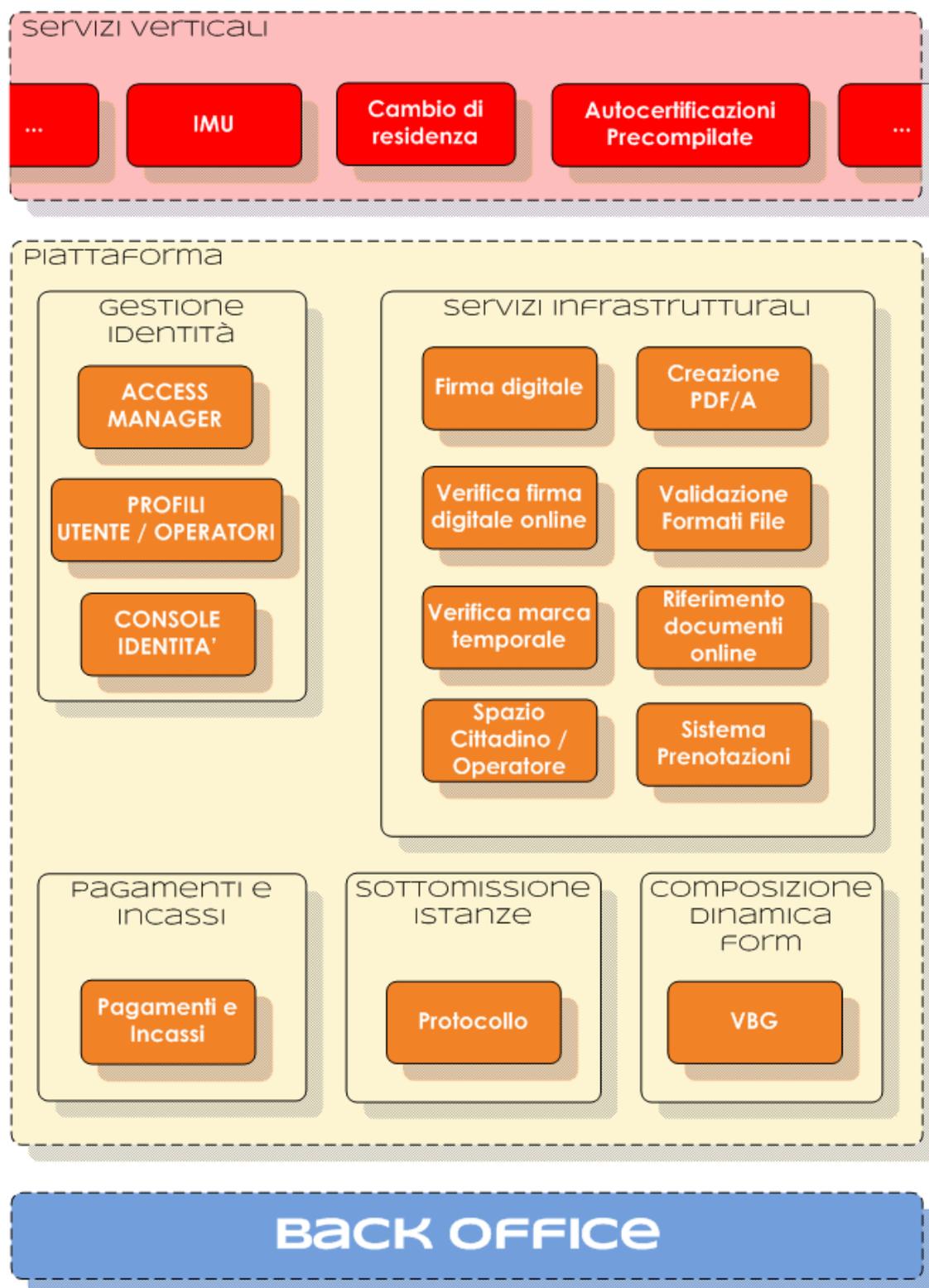


Figura 3

### 3.2. Servizi infrastrutturali

Lo scopo di questa sezione è di realizzare funzionalità di base che possano essere richiamate, tramite interfacce dati standard, da moduli di più alto livello.

Si riporta di seguito una breve descrizione di ogni modulo costituente la sezione dei servizi infrastrutturali.

### 3.2.1. Firma digitale

Il modulo “**firma digitale**” realizza un servizio interattivo di sottomissione e sottoscrizione di documenti elettronici ad uso degli operatori e dei cittadini autenticati. Permette, inoltre, la possibilità di effettuare la sottoscrizione di documenti elettronici attraverso l'invocazione di funzionalità specifiche da parte degli altri moduli del sistema.

1. Deve essere assicurato un corretto riconoscimento dei dispositivi di lettura della smartcard
2. Deve essere assicurato un corretto riconoscimento degli standard CNS/CRS inclusi i controlli previsti dalla normativa vigente
3. Deve essere possibile firmare uno o più documenti in un'unica soluzione
4. Firma molteplice di persone in ruoli differenti del documento principale e dei documenti allegati associati
5. Controllo della presenza del certificato nelle liste di revoca
6. Controllo validità scadenza del certificato

### 3.2.2. Verifica firma digitale online

Il modulo “**verifica firma digitale online**” realizza un servizio interattivo, per gli operatori ed i cittadini autenticati, di sottomissione e verifica di documenti elettronici sottoscritti, visualizzazione/estrazione dei dati di sottoscrizione, estrazione del documento elettronico contenuto e sua visualizzazione (ove possibile)

1. Ad uso degli operatori ed eventualmente dei cittadini autenticati, deve essere assicurato un servizio di:
  - a. Sottomissione interattiva di documenti elettronici sottoscritti
  - b. Verifica della firma elettronica
  - c. Visualizzazione ed estrazione dei dati di sottoscrizione
  - d. Estrazione del documento elettronico contenuto e sua visualizzazione (ove possibile)
2. Ad uso dei servizi online deve essere assicurato, attraverso l'invocazione di funzionalità specifiche:
  - a. verifica di documenti elettronici sottoscritti
  - b. estrazione dei dati di sottoscrizione in formato XML
  - c. estrazione del documento elettronico contenuto

### 3.2.3. Verifica marca temporale

Il modulo “**verifica marca temporale**” realizza un servizio interattivo di sottomissione e verifica di documenti elettronici con marca temporale, visualizzazione/estrazione dei dati di marcatura; inoltre rende disponibili agli altri moduli le funzioni di verifica di documenti elettronici con marca temporale ed estrazione dei dati di marcatura in formato XML

1. Ad uso degli operatori ed eventualmente dei cittadini autenticati, deve essere assicurato un servizio di:
  - a. sottomissione e verifica di documenti elettronici con marca temporale

- b. visualizzazione/estrazione dei dati di marcatura
- 2. Ad uso dei servizi online deve essere assicurato, attraverso l'invocazione di funzionalità specifiche:
  - a. verifica di documenti elettronici con marca temporale
  - b. estrazione dei dati di marcatura in formato XML

#### 3.2.4. Spazio cittadino/operatore

Il modulo “**Spazio cittadino/operatore**” si configura come un componente software di infrastruttura in grado di gestire, in modo organizzato, uno spazio di file dedicato agli utenti registrati del sistema. La necessità di tale modulo deriva dal fatto che, nella realizzazione di servizi di E-Government, in particolare per la sottomissione di istanze per procedimenti complessi, gli allegati richiesti possono essere molteplici e di dimensioni rilevanti, tali da poter causare la necessità di dover ripetere il processo di sottomissione. Il componente software qui descritto realizza un servizio di hosting temporaneo, tramite il quale un utente registrato ha a disposizione uno spazio su disco in cui caricare, in un ordine qualsiasi, dei file binari da allegare in modo selettivo a un'istanza da sottomettere online.

1. Ciascun file caricato deve essere identificato tramite una URI univoca prodotta dal componente stesso
2. Per ciascun file caricato, il componente di hosting temporaneo di file binari deve registrare un insieme minimo di informazioni, tra cui:
  - a. l'identificativo (codice fiscale) dell'Utente Registrato che ha effettuato il caricamento del file binario
  - b. data e ora del caricamento del file binario
  - c. nome originale del file e dimensione in byte del file binario
  - d. una breve descrizione del contenuto del file (opzionale), in formato di testo libero, inserito dall'Utente Registrato
  - e. ulteriori operazioni effettuate sul file binario (invio, cancellazione, etc.)
3. Il componente realizza una API web, compatibile con gli standard web service SOAP/XML e opzionalmente REST/XML e REST/JSON, tramite la quale è possibile effettuare le seguenti operazioni minime:
  - a. richiedere l'elenco dei file binari attualmente disponibili per un determinato Utente Registrato
  - b. caricare un file binario per un determinato Utente Registrato
  - c. accedere a un file binario, identificato tramite URI, con possibilità di indicare file multipli
  - d. inviare un file binario, identificato tramite URI, a sistemi terzi con possibilità di indicare file multipli
  - e. cancellare un file binario memorizzato, identificato tramite URI, con possibilità di indicare file multipli
4. La funzione di invio di file binario, identificato tramite URI, a sistemi terzi si configura come supporto a un processo di sottomissione istanze con allegati. Alla richiesta di invio tramite richiesta effettuata tramite la API web, il componente di hosting temporaneo di file binari risponde effettuando le seguenti operazioni:
  - a. creazione di una copia del file binario identificato tramite URI in un area dedicata del file system

- b. registrazione delle informazioni ed emissione di una nuova URI identificativa della copia
  - c. risposta alla richiesta originale, con indicazione della URI di riferimento
5. Deve essere realizzata un'interfaccia web specifica da integrare nel sistema, in base alle specifiche, per l'effettuazione delle principali operazioni da parte degli Utenti Registrati. Le funzioni minime da realizzare sono:
- a. visualizzazione dell'elenco dei file binari caricati dall'Utente Registrato che ha effettuato il login (con esclusione dei file binari creati per l'invio a sistemi terzi, che devono risultare inaccessibili agli Utenti), con indicazione dello spazio assegnato residuo
  - b. caricamento (upload) assistito di un file binario, con controllo preventivo delle dimensioni e segnalazione all'Utente dell'eventuale impossibilità di effettuare il caricamento
  - c. scaricamento (download) di un file binario
  - d. cancellazione di un file binario

Non sono invece previste, per scelta, funzioni di modifica dei file binari caricati.

6. Deve essere realizzata una funzione da integrare in altre interfacce web del sistema, al fine di permettere la scelta, da parte dell'Utente Registrato, dei file binari da allegare ad una specifica istanza. Tale funzione deve essere realizzata in modo da essere massimamente modulare e riutilizzabile in altri servizi

### 3.2.5. Creazione PDF/A

Il modulo “**Creazione PDF/A**” si configura come un componente software di infrastruttura in grado di generare file PDF, con capacità minima di generazione del formato PDF/A. L'uso principale inteso per il componente è la conversione di moduli compilati online in un formato adatto alla trasmissione, la lettura e la conservazione.

1. Il componente realizza una API web, compatibile con gli standard web service SOAP/XML e opzionalmente REST/XML e REST/JSON, tramite la quale è possibile richiedere il render di un file XML ottenendo in risposta un file binario nel formato previsto
2. Il componente deve essere in grado di produrre file PDF almeno versione 1.4, come minimo nel formato PDF/A-1
3. Preferibilmente, il componente dovrebbe essere in grado di produrre anche file PDF in versioni superiori a 1.4, secondo lo standard PDF/A-2

### 3.2.6. Validazione formati file

Il modulo “**Validazione formati file**” si configura come un componente software di infrastruttura in grado di ricevere file in formato binario e restituire una descrizione del formato tecnico effettivamente identificato, estraendo le meta-informazioni contenute nel file stesso e restituendole in un formato standard.

1. Il modulo realizza una API web, compatibile con gli standard web service SOAP/XML e opzionalmente REST/XML e REST/JSON, tramite la quale è possibile richiedere l'analisi di un file in formato binario ottenendo in risposta un file XML di descrizione
2. Per maggiore flessibilità di integrazione, deve inoltre essere possibile trasmettere al componente il file binario in uno qualsiasi di almeno questi modi:
  - a. embedding diretto nella richiesta
  - b. URL verso un sistema terzo
  - c. percorso nel file system
3. Dovrebbe essere possibile richiedere l'analisi di più file binari con una sola richiesta
4. Come minimo, il componente di verifica del formato dei file binari deve essere in grado di estrarre le meta-informazioni contenute nel file stesso e restituirle in un formato standard
5. Il componente deve svolgere le funzioni sopra descritte in modo autonomo e in locale, a meno delle interazioni con sistemi terzi a scopo di integrazione

### 3.2.7. Riferimento documenti online

Il modulo “**riferimento documenti online**” si configura come un componente software di infrastruttura in grado di gestire in modo organizzato l'accesso a file binari prodotti dagli Enti, da parte di utenti ed utenti registrati.

1. Ciascun file reso disponibile deve essere identificato tramite una URI univoca prodotta dal componente stesso
2. Per ciascun file inserito, il componente di gestione dell'accesso esterno a file binari deve registrare un insieme minimo di informazioni, tra cui:
  - a. identificativo dell'Ente e dell'operatore che ha effettuato l'inserimento
  - b. identificativo dell'Ente e dell'eventuale unità organizzativa
  - c. data e ora dell'inserimento del file binario
  - d. nome originale del file e dimensione in byte del file binario
  - e. eventuale identificativo dell'Utente Registrato (codice fiscale) cui è riservato l'accesso
  - f. stringa descrittiva di testo
  - g. stringa di taggatura del file
  - h. ulteriori operazioni effettuate sul file binario (accesso, cancellazione)
3. Il modulo realizza una API web, compatibile con gli standard web service SOAP/XML e opzionalmente REST/XML e REST/JSON, tramite la quale è possibile effettuare le seguenti operazioni minime:
  - a. ricercare i file binari
  - b. richiedere l'elenco dei file binari inseriti disponibili per un determinato Utente Registrato
  - c. inserire un file binario per un determinato Utente Registrato
  - d. accedere a un file binario
  - e. cancellare un file binario memorizzato

4. Deve essere possibile costruire una URL standard di riferimento a ciascun file binario, a partire dalla URI identificativa. Tale URL ha la funzione di permalink, da includere eventualmente in altre pubblicazioni
5. Deve essere realizzata un'interfaccia web specifica, da integrare nel sistema, per l'effettuazione delle principali operazioni da parte di Utenti e Utenti Registrati. Le funzioni minime da realizzare sono:
  - a. *ricerca* di file binari non riservati a specifici Utenti Registrati
  - b. *visualizzazione* dell'elenco dei file binari riservati all'Utente Registrato che ha effettuato il login
  - c. *visualizzazione* diretta della *descrizione* di un file binario a partire da URL (pagina di atterraggio); la funzione deve richiedere la login preventiva se il file binario è riservato a un Utente Registrato; il file binario deve essere direttamente scaricabile
6. Deve essere realizzata un'interfaccia web specifica da integrare nel sistema, per la gestione manuale dei file inseriti per gli Operatori di back-office degli Enti. Le funzioni minime da realizzare sono:
  - a. *ricerca* di file binari inseriti da un particolare Ente, con eventuale indicazione dell'unità organizzativa
  - b. *inserimento* di un file binario con indicazione delle informazioni necessarie e la selezione assistita dell'Utente Registrato cui il file binario è riservato
  - c. *cancellazione* di un file binario precedentemente inserito

### 3.2.8. Sistema prenotazioni

Il modulo “**Sistema prenotazioni**” si configura come un sistema in grado di gestire la disponibilità e le prenotazioni per un insieme di *risorse prenotabili* generiche e modificabili dinamicamente, nel corso delle attività. Ciascuna risorsa prenotabile è associata a un calendario di disponibilità per la prenotazione, che definisce il periodo di disponibilità con dettaglio giornaliero, oltreché la durata minima e massima della prenotabilità e l'eventuale possibilità di uso contemporaneo.

1. Ciascuna risorsa prenotabile deve essere identificabile attraverso una URI univoca definita dal sistema e deve avere le seguenti caratteristiche descrittive minime:
  - a. deve essere riconducibile a uno e un solo Ente partecipante
  - b. deve essere riconducibile a una unità organizzativa dell'Ente
  - c. deve poter essere associata ai dati di un Operatore di Back-Office che ne è il referente per conto dell'Ente
  - d. deve poter essere associata a un testo descrittivo in formato HTML, che può includere eventuali riferimenti ad altra documentazione online
  - e. dovrebbe poter essere associata a un testo di avvertenze per l'Utente, da riportarsi in ciascuna comunicazione
2. Ciascuna risorsa prenotabile deve essere associata a un calendario di disponibilità per la prenotazione, che definisce:
  - a. un periodo di disponibilità
  - b. una disponibilità giornaliera di dettaglio, organizzata per settimane e mesi, con la possibilità di definire eccezioni, come festività e/o periodi di indisponibilità

- c. le caratteristiche dell'oggetto di ciascuna singola prenotazione, in termini di durata minima e massima e della granularità temporale di inizio e fine
  - d. quante prenotazioni possono al massimo essere sovrapposte
- 3. Per ciascuna risorsa prenotabile deve essere possibile specificare:
  - a. se la risorsa è prenotabile solo da Utenti Registrati o da tutti gli Utenti (gli Utenti Registrati potranno accedervi in ogni caso)
  - b. se è consentita la prenotazione per conto di altre persone o di più persone
 Dovrebbe essere inoltre possibile specificare:
  - c. se le prenotazioni richiedono la conferma da parte del referente o da parte di un sistema automatico esterno
  - d. se le prenotazioni possono essere modificate una volta inserite o se è solo possibile la cancellazione
- 4. Dovrebbe essere possibile definire risorse prenotabili come data unica (p.es. corsi di formazione, eventi speciali), cui è legato un unico slot e una disponibilità effettiva
- 5. Dovrebbe inoltre essere possibile registrarsi in una lista d'attesa in caso di non disponibilità dello slot unico
- 6. Un Utente o Utente Registrato deve poter effettuare le seguenti operazioni, in modalità self-service tramite interfaccia web:
  - a. visualizzare l'elenco delle risorse prenotabili di uno specifico Ente
  - b. visualizzare il testo descrittivo e delle avvertenze associate a una specifica risorsa prenotabile
  - c. visualizzare il calendario delle disponibilità della risorsa prenotabile, in modo facile, intuitivo e gradevole
  - d. selezionare uno slot disponibile
  - e. effettuare una prenotazione inserendo anche le informazioni obbligatorie e opzionali
- 7. L'avvenuta prenotazione in modalità self-service tramite interfaccia web deve essere confermata da un'apposita pagina in cui è riportato il riepilogo delle informazioni salienti, con particolare evidenza dell'identificativo, inteso come URI. La pagina dovrebbe essere predisposta per la stampa.
- 8. Tale pagina di conferma deve essere associata a una URL per la visualizzazione successiva
- 9. La URL di visualizzazione dovrebbe essere riportata sulla pagina anche come QR Code
- 10. Gli spazi corrispondenti ad una prenotazione cancellata dovrebbero essere rimesse in disponibilità per gli altri utenti
- 11. Se la risorsa prenotabile lo consente, l'Utente dovrebbe poter modificare la propria prenotazione utilizzando la URL indicata nella pagina di conferma e nell'email
- 12. Gli spazi non più prenotati a seguito della modifica dovrebbero essere rimesse in disponibilità per gli altri utenti
- 13. All'atto della visualizzazione, la pagina deve riportare in modo evidente anche lo stato (inteso come: in attesa di conferma, confermata, cancellata)
- 14. Un Operatore di Back Office deve poter gestire le prenotazioni effettuate per ciascuna risorsa prenotabile tramite interfaccia web. In particolare, l'interfaccia web deve permettere le seguenti operazioni:

- a. selezione di una risorsa prenotabile da un elenco di risorse cui l'Operatore ha accesso
  - b. visualizzazione delle prenotazioni effettuate e attive per una risorsa prenotabile selezionata, con la possibilità di vedere le prenotazioni per slot (da calendario), in ordine cronologico o effettuando una ricerca per cognome dell'Utente
  - c. visualizzazione delle prenotazioni in attesa di conferma (se previsto per quella risorsa) e delle prenotazioni cancellate
  - d. effettuazione di una prenotazione per conto di un Utente
  - e. conferma o cancellazione di una prenotazione in attesa di conferma
  - f. cancellazione di una prenotazione effettuata
15. Un Operatore di Back Office deve poter creare nuove risorse prenotabili, tramite un'interfaccia web semplice ed intuitiva
  16. Tramite interfaccia web, un Operatore di Back Office deve poter modificare le caratteristiche di una risorsa prenotabile attiva
  17. Il sistema dovrebbe avere un metodo (p.es. procedura temporizzata) per recuperare la disponibilità di prenotazioni comunque non completate (p.es. abbandono o perdita della connessione)
  18. Il modulo realizza una API web, compatibile con gli standard web service SOAP/XML e opzionalmente REST/XML e REST/JSON, tramite la quale è possibile effettuare il recupero dell'elenco di prenotazioni relative a un determinato Utente Registrato, identificato per codice fiscale, con possibilità di indicare un periodo temporale e/o un vincolo sulle risorse prenotabili (in termini di Ente e/o di unità organizzativa)
  19. Il sistema per la gestione delle risorse prenotabili realizza funzioni di notifica agli Utenti e Utenti registrati e a Operatori di back-office degli eventi relativi alle istanze inserite. Le notifiche vengono inviate tramite email e/o SMS, attraverso sistemi gateway terzi
  20. Come minimo devono essere previste notifiche all'Utente o Utente registrato in corrispondenza dei seguenti eventi:
    - a. inserimento di una prenotazione
    - b. conferma di una prenotazione (se prevista)
    - c. modifica di una prenotazione (se consentita)
    - d. cancellazione di una prenotazione

Copia delle notifiche deve essere inviata anche agli Operatori di back-office i cui indirizzi sono associati alla risorsa prenotabile coinvolta

### 3.3. Gestione identità

I moduli della sottosezione “**gestione identità**” (“**access manager**”, “**profili utente/operatori**”, “**console identità**”) realizzano la completa gestione delle informazioni che costituiscono il profilo di una persona fisica, dal processo di creazione e organizzazione, fino all'eliminazione dell'identità digitale.

Ogni singola persona, dispone di una o più identità digitali secondo specifici ruoli di:

- cittadino/professionista (identità unica)
- operatore di Ente

Grazie a tali moduli ciascuna di queste identità digitali viene attivata o disattivata secondo un predeterminato ciclo di vita.

### 3.3.1. Gestione integrata operatori di back-office

Va sottolineato che, a differenza degli account dei cittadini (vedi sotto), gli account degli operatori sono autorizzati ad agire per conto di un solo Ente. Ciascun Ente ha un proprio responsabile incaricato.

Ciò detto, le strutture dati di riferimento descrittive della gestione integrata degli operatori di back office permettono di gestire gli account e le autorizzazioni dei singoli operatori.

### 3.3.2. Gestione integrata dell'identità dei cittadini

I cittadini utenti del sistema possono essere dotati di credenziali di accesso online valide su base nazionale (tipicamente *smartcard* tipo CNS/CRS) ovvero essere dotati di credenziali a valore più limitato, emesse da Enti o aggregazioni di Enti.

La gestione integrata dell'identità dei cittadini del sistema è in grado di utilizzare tutte e due le modalità previste dalla normativa.

L'emissione di credenziali specifiche per l'uso con il sistema, nello specifico una coppia username/password prevede i seguenti passi:

- 1) compilazione online, da parte del cittadino o di un operatore, di un modulo contenente informazioni adeguate all'identificazione e al contatto;
- 2) identificazione diretta ('de visu') del cittadino, con presentazione di un documento ad un operatore autorizzato e consegna di una password in busta chiusa e sigillata;
- 3) attivazione dell'account del cittadino (la username coincide con il codice fiscale) e attivazione della password contenuta nella busta e dotata di un identificatore 'pubblico' stampato all'esterno.

Successivamente le credenziali sono attive e possono essere utilizzate per tutte le funzioni presso qualsiasi Ente avente un'area servizi ospitata nel sistema.

Le funzioni applicative per la gestione integrata dell'identità dei cittadini hanno lo scopo di permettere lo svolgimento delle funzioni di cui sopra.

Il software consiste in una suite di applicativi web realizzate come Vaadin e Java Servlet, pagine JSP e personalizzazioni delle funzioni di Access manager OpenAM. Gli applicativi utilizzano il DBMS MySQL.

### 3.3.3. Gestione integrata delle smartcard (CNS, CRS)

Il sistema, in base alle già citate normative vigenti, consente l'uso della CNS/CRS e permette di effettuare il processo di registrazione online senza dover effettuare l'identificazione diretta presso un punto di registrazione autorizzato. Al cittadino viene comunque offerta la possibilità di avere credenziali ulteriori, come username e password, al fine di facilitare l'accesso tramite dispositivi non in grado di leggere e integrarsi con le smartcard.

L'applicativo, che estende il sistema di gestione integrata dell'identità dei cittadini, è stato realizzato come applicazione web stand alone (Vaadin e Java Servlet), pagine JSP e personalizzazioni delle funzioni di Access manager OpenAM.

### 3.4. Pagamenti e incassi

Il “Modulo pagamenti ed incassi” si configura come un payment gateway che può funzionare in modalità multiservizio e multiente, instradando i pagamenti effettuati dai cittadini verso i sistemi di POS virtuale attivati dai singoli Enti. Nell’ambito della soluzione saranno rilasciati a riuso i plugin per il colloquio con i seguenti circuiti bancari di pagamento:

- CartaSi
  - Unicredit
  - Intesa San Paolo
1. Vengono gestite le funzioni di rendicontazione, logging e di amministrazione pagamenti da parte degli Enti
  2. Il modulo dovrà essere strutturato a “plugin”, i quali dovranno interagire con sistemi di pagamento di terze parti
  3. Ogni plugin realizza sulla base di software creato ad-hoc gli scambi dei flussi informativi con il rispettivo circuito bancario

### 3.5. Sottomissione istanze

Il “Modulo sottomissione istanze” si configura come un componente di infrastruttura per la gestione delle istanze da sottomettere al back-office degli Enti. In particolare, il sistema di sottomissione istanze si incarica di gestire la fase di transizione che va dal completamento dell’inserimento dell’istanza, tramite servizi specifici realizzati da altri componenti software, e la presa in carico da parte degli Enti.

Ciascuna istanza è composta da uno o più file binari, eventualmente firmati digitalmente, ed è riconducibile a un Utente o un Utente registrato.

Le istanze vengono gestite dal sistema come copia primaria solo nel periodo che va dal completo inserimento fino alla presa in carico da parte dell’Ente. Per questo motivo, pur essendo necessaria la massima cura al fine di garantire l’integrità dell’istanza, al sistema di sottomissione istanze non si applicano gli obblighi per la conservazione di lungo periodo previsti dalla normativa vigente per le pubbliche amministrazioni.

La principale funzione del sistema è l’interfacciamento con i sistemi di protocollo del back-office degli Enti. Il sistema realizza anche un’interfaccia web dedicata agli Operatori di back-office al fine di gestire l’inserimento manuale e/o di emergenza delle informazioni di protocollo.

1. Il sistema deve essere in grado di garantire l’integrità dei file binari e della loro aggregazione durante la fase di trasmissione
2. Ciascuna istanza è indirizzata ad uno ed un solo Ente ed è riconducibile (come inserimento) a uno ed un solo Utente o Utente registrato
3. Ciascuna istanza deve essere identificata tramite una URI univoca prodotta dal sistema
4. Per ciascuna istanza caricata, il sistema di sottomissione istanze deve registrare un insieme minimo di informazioni, tra cui:
  - a. l’identificativo (codice fiscale) dell’Utente Registrato o comunque dell’Utente che ha effettuato l’inserimento
  - b. una stringa descrittiva del tipo di istanza inserita
  - c. data e ora del caricamento del file binario

- d. elenco dei file binari presenti nell'aggregazione
  - e. data e ora del trasferimento con presa in carico dell'istanza da parte dell'Ente
  - f. dati di protocollo definiti dall'Ente al momento della presa in carico
5. Il modulo realizza una API web, compatibile con gli standard web service SOAP/XML e opzionalmente REST/XML e REST/JSON, tramite la quale è possibile effettuare le seguenti operazioni minime:
    - a. richiedere l'elenco delle istanze inserite per un determinato Utente o Utente Registrato
    - b. richiedere l'elenco delle istanze inserite per un determinato Ente
    - c. inserire un'istanza per un determinato Utente o Utente Registrato ed un Ente
    - d. accedere alle informazioni memorizzate e/o ai file binari di una particolare istanza
    - e. comunicare la presa in carico di un'istanza, indicando i dati di protocollo
  6. Il sistema di sottomissione istanze realizza funzioni di trasmissione delle istanze inserite agli Enti destinatari. La trasmissione delle istanze può avvenire in tre modi diversi:
    - a. *Automatico, sincrono*  
Il sistema di sottomissione istanze chiama un sistema terzo dell'Ente inviando l'istanza completa dei file binari e ricevendo i dati di protocollo in risposta
    - b. *Automatico, asincrono*  
Il sistema di sottomissione istanze attende la chiamata da parte di un sistema terzo dell'Ente e riceve i dati di protocollo a seguito della presa in carico
    - c. *Manuale e/o di emergenza*  
Il sistema di sottomissione istanze, attraverso un'interfaccia web specifica, permette a un Operatore di back-office di visualizzare la lista delle istanze non ancora prese in carico, di scaricare le informazioni e i file binari di istanze specifiche e di inserire (manualmente) i dati di protocollo che attestano la presa in carico
  7. Deve essere possibile configurare la modalità di trasmissione delle istanze in modo indipendente per ciascun singolo Ente e per ciascuna tipologia di istanza
  8. Deve essere possibile integrare nel sistema molteplici *plugin*, corrispondenti a sistemi diversi
  9. Deve essere inoltre possibile indicare quale *plugin* e configurazione utilizzare per la trasmissione *sincrona* di istanze, in base all'Ente destinatario e la tipologia

### 3.6. Composizione dinamica form

Il sistema dovrà prevedere delle funzionalità che diano la possibilità di modellare l'iter del servizio, le informazioni gestite con i relativi vincoli ed il flusso di interazione con l'utente.

1. Sarà implementata una gestione evoluta degli allegati in grado di integrarsi con il servizio documenti riferimenti online, per superare le limitazioni dell'attuale piattaforma People di erogazione dei servizi
2. Sarà previsto un sistema agile di esposizione dei servizi modellati con le funzioni suddette
3. Per servizi di questa natura, sarà prevista una funzionalità per il salvataggio delle informazioni nelle fasi intermedie di compilazione e per il recupero dello stato

### **3.7. Servizi verticali**

Verranno realizzati tre componenti software sperimentali dedicati a specifici servizi online di e-Government che utilizzano l'insieme di interfacce e di standard evidenziati nell'ambito della soluzione tecnica proposta.

#### **3.7.1. IMU**

Questa applicazione permette di calcolare l'ammontare dell'IMU secondo il D.L. 201/2011, convertito in Legge con modificazioni dalla L. 214/2011.

Per il calcolo dell' IMU sarà sufficiente selezionare il gruppo o la categoria catastale cui appartiene l'immobile e inserire la relativa rendita catastale non rivalutata (per i terreni agricoli è il reddito dominicale non rivalutato).

In prima forma (si escludono casi particolari, per i quali si rimanda alle pratiche di sportello), il servizio, si baserà su tutta una serie di informazioni di base precompilate dagli Enti locali e offrirà in modo quanto più possibile automatizzato le somme calcolate al cittadino.

#### **3.7.2. Cambio di residenza**

Verrà realizzato il servizio online di cambio di residenza sulla base della normativa anagrafica vigente ovvero sulle specifiche emanate all'interno del nuovo regolamento anagrafico.

#### **3.7.3. Autocertificazioni precompilate**

Il servizio prevede autenticazione, e si articola attraverso la precompilazione con i propri dati anagrafici e qualora disponibili quelli aggiuntivi parte del "profilo arricchito" (p.es. Titolo di studio, professione, etc.) di autocertificazioni standard (rese disponibili in formato pdf/a ed anche in formato testo per un agevole riutilizzo).

Questo servizio viene a rispondere alle esigenze maturate dal nuovo assetto normativo che prevede una significativa decertificazione.

### **3.8. Adattabilità della soluzione**

La soluzione per l'erogazione dei servizi può essere inserita in un contesto più ampio, come ad esempio un centro servizi territoriale (CST) o un'alleanza locale per l'innovazione (ALI), deve quindi essere progettata in modo tale che possa interfacciarsi con altri componenti che non fanno parte della presente progettualità quali ad esempio:

- gestione dei contenuti informativi
- piattaforme di social media networking
- reportistica
- contact center
- smartphone e tablet
- area servizi: user integration per concentrare i contenuti di diversa natura in un'unica interfaccia di interazione

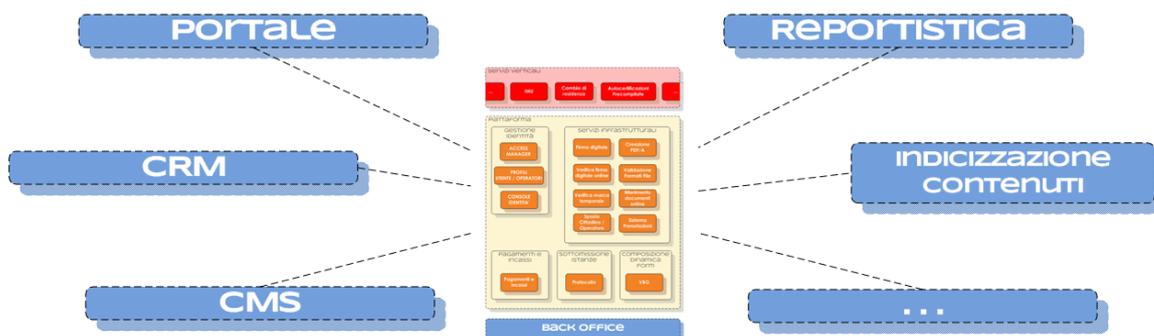


Figura 4

## 4. Architettura tecnica

---

Il presente capitolo ha lo scopo di evidenziare la correlazione tra le funzionalità dei prodotti FLOSS selezionati e dei servizi infrastrutturali progettati e integrati nella piattaforma PEOPLE LPCE.

Si rende noto che la numerosità dei server non è determinabile a priori ma occorre analizzare appieno le esigenze dei diversi contesti di destinazione che possono, per ogni Ente, essere mutevoli.

I livelli diagrammati: Front End, Back End e Banche Dati corrispondono anche ad un'architettura di rete strutturata su tre distinti livelli, i quali si compongono di:

- un primo livello di interazione con il cittadino / operatore, verifica il contenuto informativo della richiesta, normalizza la richiesta stessa e la inoltra verso il server applicativo collocato nel secondo livello
- un secondo per il dispiegamento delle applicazioni, quindi di elaborazione dati, detto anche di middleware
- un terzo, con accesso consentito esclusivamente ai server presenti nel livello di middleware, che gestisce la memorizzazione delle informazioni delle applicazioni software e le credenziali degli utenti

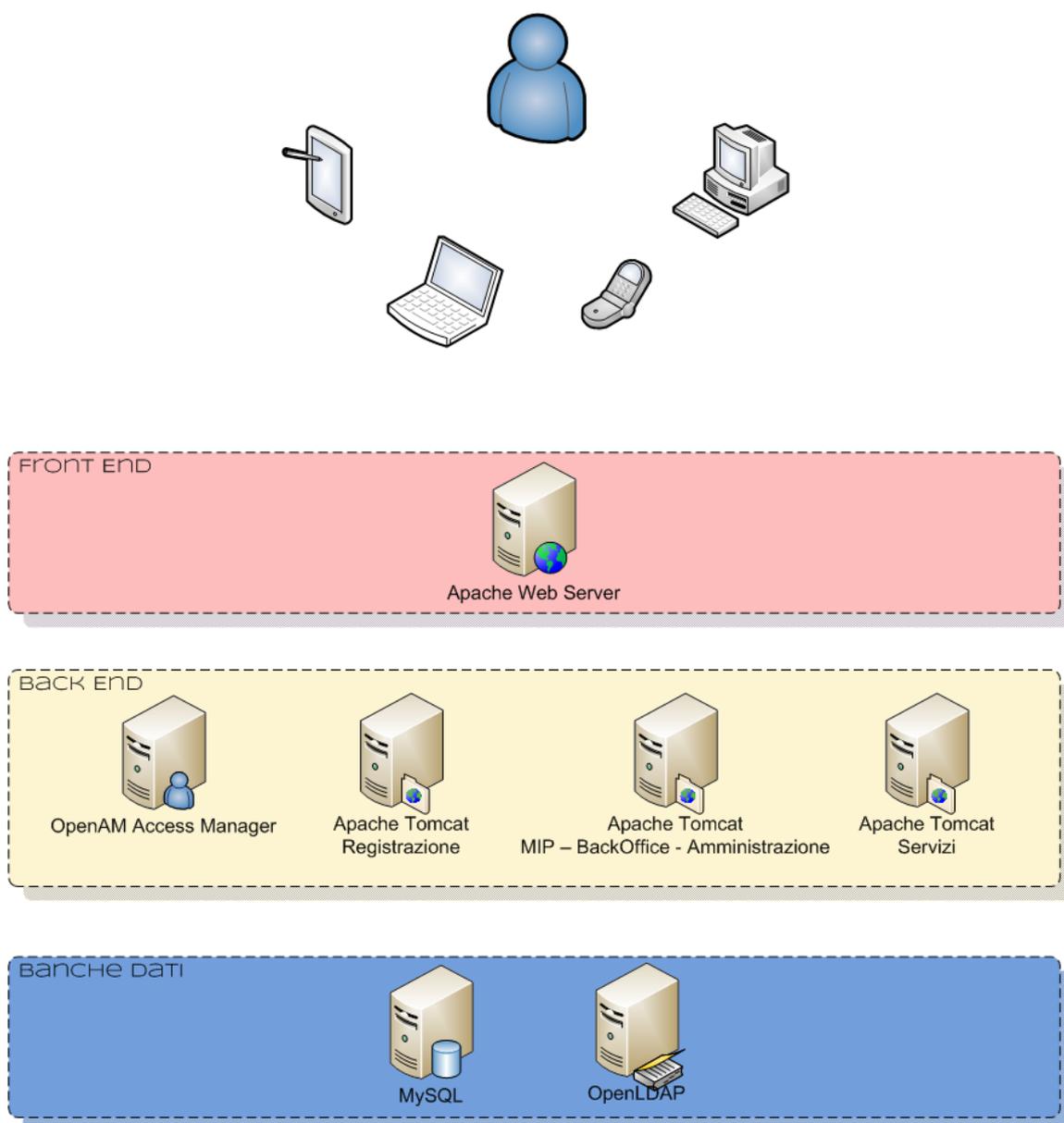


Figura 5

La Figura 5 descrive tre tipi di informazione:

1. infrastruttura hardware e di virtualizzazione
2. architettura di rete
3. architettura software di base

I livelli 1 e 2 costituiscono un prerequisito e di seguito vengono descritti gli elementi essenziali che sono assunti come ipotesi di lavoro per poter dare la definizione della soluzione complessiva.

Il livello 3, invece, costituisce la base delle componenti software e delle loro interazioni in riferimento alla quale viene definita la modalità di realizzazione e dispiegamento dei servizi.

## 4.1. Stack tecnologico di riferimento

Si rende noto che lo stack tecnologico e i prodotti di riferimento selezionati che compongono la struttura della piattaforma nel suo complesso, sono i seguenti:

### Sistema e ambiente operativo

- Linux, distribuzione Debian vers. 6.x

### Middleware

- Web Server: Apache HTTP Server vers. 2.2
- Access Manager: OpenAM vers. 9.x + OpenLDAP 2.4+
- Interprete Bytecode e Servlet Engine: Java VM 1.6+, Apache Tomcat 6.x
- Interfacce: Apache CXF e Spring (standard SOAP/XML, REST/XML, REST/JSON)
- Presentazione (front end): Java Vaadin (costruzione moduli online)

### Database

- MySQL, vers. 5.1+

## 4.2. Piattaforma

### 4.2.1. Gestione dell'identità

La gestione dell'identità è strutturata secondo il seguente insieme di componenti:

1. Access Manager
2. Memorizzazione profili
3. Console di Registrazione

L'insieme delle parti, lavora di concerto e offre tutte le funzionalità per garantire la gestione dei dati del profilo a norma del Codice dell'Amministrazione Digitale.

I primi due componenti sono software infrastrutturali e offrono possibilità di:

- Federazione con sistemi terzi
- Estensione della sicurezza del SSO (Single SignOn) locale e remota a domini terzi (Centri Servizi, ALI)
- Recupero identità e attributi dei profili utente
- Intermediari ruoli e deleghe tramite predisposizione integrazione sistemi terzi basata su profilo dinamico
- Creazione e conservazione delle credenziali
- Consegna credenziali in modalità sicura
- Integrazione piattaforme di social media network (p.es. Facebook, Twitter) e prodotti terzi p.es. Content Management System (CMS)
- Espandibilità basata su plugin (p.es. logica MIP)

#### 4.2.1.1. Access Manager OpenAM

OpenAM è una soluzione software Open Source (CDDL Licensing) per la gestione delle problematiche sugli accessi ai sistemi informatici per consentire qualsivoglia politica di sicurezza.

Nata inizialmente da SUN Microsystems è stata rilasciata in versioni successive di pubblico dominio. In seguito è stata rilevata da ForgeRock che attualmente la manutiene, la estende e la supporta (comprese le parti documentali reperibili direttamente in rete).

ForgeRock propone anche programmi specifici di formazione.

OpenAM è il “motore” centrale per la gestione degli accessi locali e remoti e supporta i seguenti protocolli (standard industriali) aperti:

- SAML1.1 e 2.0
- ID-FF 1.2
- WS-Federation 1.1
- ID-WSF 1.1
- WS-Security (WS-I BSP)
- OAuth 1.0 e 2.0
- JDBC
- RADIUS
- Active Directory
- Unix
- HTTP\_Basic
- LDAP

OpenAM è basato sullo standard Java Authentication and Authorization Service (JAAS) e consente di estenderne le funzionalità attraverso una struttura configurabile a “plugin” denominata “login module” che attua il meccanismo d’autenticazione desiderato:

- Busta username/password
- Smartcard (p.es. Carta Nazionale dei Servizi),
- OTP/RSA,
- Database

E’ possibile creare, qualora non inclusi nel prodotto base, ulteriori plugin tramite estensione di un’interfaccia per la quale è prevista e documentata sul sito ForgeRock un set specifico di API.

Fra le caratteristiche di rilievo (modalità accertamento identità pre-erogazione servizio) è possibile stabilire un utilizzo in cascata dei meccanismi di autenticazione citati (authentication chain). Per esempio qualora all’accesso la carta nazionale dei servizi non sia verificata, il sistema “scala” in modo automatico alla successiva modalità configurata, per esempio busta username/password.

E’ possibile interfacciarsi a sistemi federati terzi come ad esempio i sistemi regionali. In questo caso, il supporto dello standard industriale SAML rappresenta sia la “predisposizione” sia il limite con cui viene rilasciata la presente soluzione. La configurazione del SAML è condizione necessaria ma non è detto che sia sufficiente; spesso, è necessario configurare il protocollo e in aggiunta ricorrere all’utilizzo di plugin realizzati ad-hoc che elaborano, nelle fasi successive, l’avvenuta identificazione, in modalità federata, e le

logiche di associazione degli attributi del profilo (non è detto vi sia pari molteplicità o medesima denominazione degli attributi tra piattaforme diverse).

E' utilizzato per offrire funzionalità di Single Sign On (SSO) per le applicazioni locali. Si può utilizzare un'ulteriore modalità semplificata (rispetto a standard come SAML) che consente l'estensione del Single Sign On a sistemi di dominio remoti tramite l'installazione di plugin rilasciati con il prodotto per server web di mercato quali: Apache Web Server, Internet Information Server e Servlet engine quali: Tomcat, Websphere, JBoss.

L'architettura del prodotto è particolarmente modulare per accogliere le diverse possibili esigenze, non occorre aggiungere ulteriori componenti per completare l'espletamento delle funzionalità citate.

Il prodotto consente di veicolare i dati di identità tra piattaforma locale e piattaforme remote, come quelle ad esempio di altri Enti o di social network.

L'esperienza del Centro Servizi del Comune di Firenze, ha visto l'interfacciamento degli Enti partecipanti con servizi di SSO remoto e connettività federata con i sistemi ARPA della Regione Toscana.

Ad esempio pratico, l'utente è identificato una tantum dai sistemi regionali e naviga con continuità e trasparenza sui servizi offerti dal Centro Servizi del Comune di Firenze e su quelli erogati localmente dalle piattaforme degli Enti Locali connessi in altra modalità (SSO remoto tramite utilizzo di Agent).

Un'altra funzione chiave è la possibilità di avere, per ogni canale, gruppi utenti diversi. Questa è realizzata utilizzando il concetto di "realm", attraverso il quale si ottengono link web di interfacciamento alla piattaforma costituiti da un prefisso comune ma da un suffisso formato in modo differente.

Ogni applicazione software può interfacciarsi al sistema in modalità web, soap/xml, rest/xml, rest/json, librerie java (API).

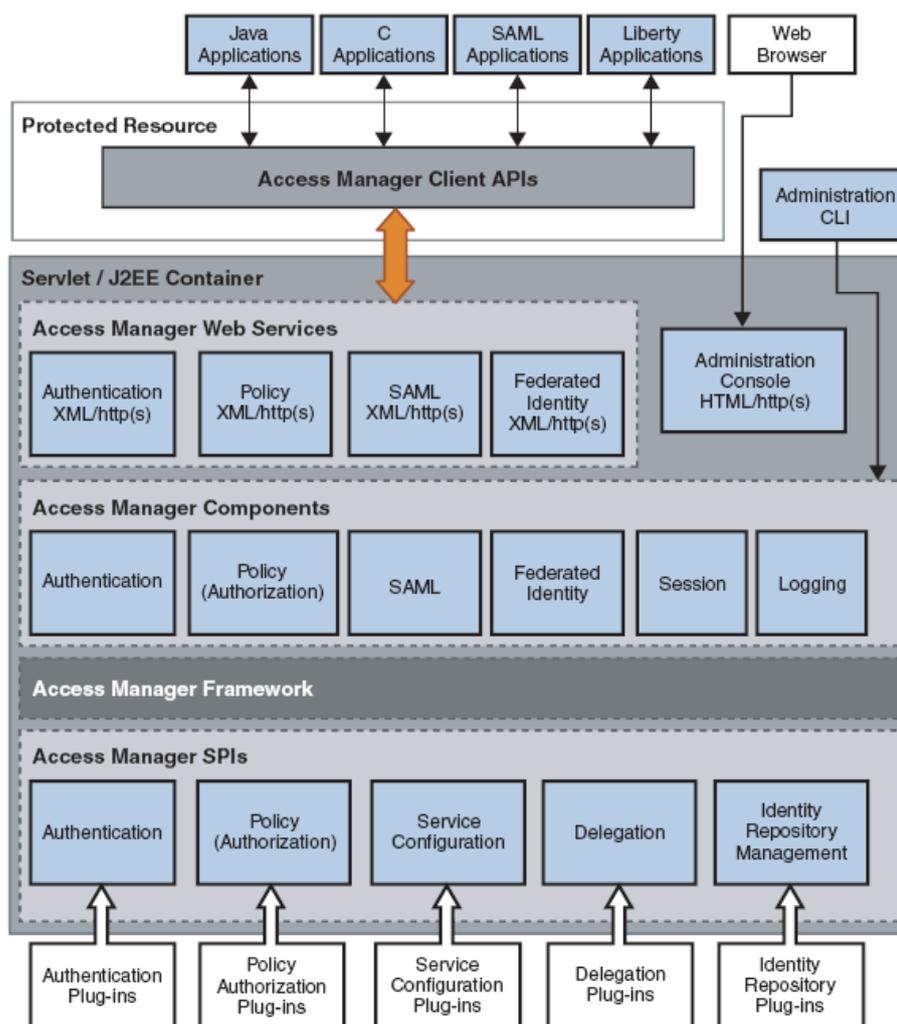


FIGURE 1-4 Access Manager Internal Architecture

Figura 6

È così possibile ottenere il profilo completo dell'identità dell'utente piuttosto che la semplice e limitata risposta di avvenuta o non avvenuta autenticazione come invece avviene nei sistemi CAS.

#### 4.2.1.2. Memorizzazione profili utente OpenLDAP

OpenLDAP è una implementazione libera, open source del Lightweight Directory Access Protocol (LDAP). È stato rilasciato mediante una propria licenza in stile BSD denominata "OpenLDAP Public License". LDAP è un protocollo indipendente dalla piattaforma ed è incluso in tutte le più diffuse distribuzioni Linux che includono il software OpenLDAP per supportare LDAP.

Questo software funziona anche su altri sistemi operativi: BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows (NT e derivati), e z/OS. Il progetto iniziale risale al 1998, a garanzia del suo consolidato livello di maturità ed a risposta del perché è ampiamente diffuso.

Il software OpenLDAP è formato da tre componenti principali:

- slapd , cioè il demone LDAP vero e proprio con i relativi strumenti di controllo

- le librerie che implementano il protocollo LDAP e le BER - ("Basic Encoding Rules")
- le regole di codifica per il linguaggio ASN.1

Dispone a corredo di software client per la gestione, l'interrogazione e la manutenzione del database: ldapsearch, ldapadd, ldapdelete, ldapmodify. Oggi sono disponibili strumenti web, anch'essi FLOSS, che offrono le medesime funzioni di gestione tramite interfaccia grafica.

Il progetto OpenLDAP ha dato l'avvio, nel tempo, ad alcuni sottoprogetti per l'interfacciamento che hanno prodotto una serie di componenti software che lo completano:

- JLDAP - librerie di classi LDAP per Java
- JDBC-LDAP - driver di collegamento tra LDAP e le librerie JDBC
- ldapc++ - librerie di classi LDAP per il C++

Il beneficio principale nell'uso LDAP è il consolidamento di certi tipi di informazioni che assolvono alle funzioni di:

1. memorizzazione dei profili utente con attributi differenziati per tipologia utenti, secondo necessità
2. policy di sicurezza specifiche per gli attributi del profilo utente
3. integrazione con prodotti terzi (vds. rif. Figura 6)
4. directory strutturata distribuita (p.es. tra Enti della PA diversi)

Per quanto concerne il primo punto in elenco sono stati ritenuti fondamentali, ai fini della corrente progettualità, il consolidamento e la diffusione della tecnologia, ampiamente documentata e i tempi di risposta del prodotto (vds. Appendice 2).

La molteplicità di possibili parametrizzazioni delle configurazioni di policy per la sicurezza ha consentito di poter associarne alcune che si riportano di seguito a titolo esemplificativo:

- password di 8 caratteri alfanumerici misti
- blocco automatico dopo 15 tentativi di accesso non andati a buon fine per un'ora

Il riconoscimento sul mercato dello standard industriale LDAP consente l'integrazione "nativa" (funzionalità di integrazione già presenti nei prodotti, senza necessità di dover ricorrere ad attività di system integration realizzate ad-hoc) con prodotti terzi come ad esempio i CMS (Content Management System) gli ambienti di portali, le soluzioni di reportistica di business intelligence e i server di posta elettronica.

In ultimo si evidenzia il beneficio e la semplificazione offerti dalla tecnologia LDAP per realizzare sistemi federati (paragonata a X.500 e SAML) e la coerenza delle sue API. Ciò significa che per alcune realtà laddove è presente una rete telematica regionale "sicura" realizzare un sistema federato, senza necessità di ridondare i dati dei cittadini, si può e con costi più modesti.

Nella progettualità corrente le uniche applicazioni che si interfacciano direttamente al prodotto OpenLDAP sono le console (applicazioni software web) che partecipano ai processi di gestione del profilo cittadino e operatore. Successivamente le informazioni sono recuperabile tramite gli ulteriori standard industriali a protocolli messi a disposizione dal prodotto OpenAM (Access Manager).

#### **4.2.1.1. Console di Registrazione**

Dovrà essere possibile centralizzare le informazioni inerenti i profili utente.

Dovrà essere garantita l'aderenza alla normativa (CNS, CRS) ed agli standard tecnologici (LDAP3.x, SAML2.x).

I processi di assegnazione delle credenziali dovranno essere conformi alla normativa C.A.D.

Dovrà essere possibile effettuare accesso in lettura alle informazioni tramite diverse tecnologie: Web Service, REST, API

I profili degli utenti dovranno essere recuperati direttamente dalla componente di Identity Management, in modo tale da garantire la centralità del profilo utente.

#### **4.2.2. Pagamenti e Incassi**

Il modulo pagamenti e incassi (MIP) è ereditato dal progetto PEOPLE e utilizzato "as-is" nell'architettura della soluzione PEOPLE LPCE.

Il software è Open Source e rilasciato con licenza GPL e iscrivibile a catalogo riuso.

Consente le principali funzionalità per la gestione dei pagamenti e degli incassi, meglio descritte in seguito, inclusa la possibilità di analisi degli storici. Dispone inoltre di un'interfaccia di integrazione, per servizi esterni al Modulo pagamento e Incassi (MIP), siano essi Servizi People o Servizi non-People, opportunamente standardizzata, attraverso la quale può essere efficacemente integrato con sistemi terzi.

Il modulo principale per la corretta gestione dei flussi di pagamento può utilizzare, a prescindere dalla modalità, una serie di circuiti bancari. La struttura (architettura) software gestisce per ottemperare allo scopo, plugin specifici per ogni circuito bancario previsto.

Nel tempo gli Enti di PP.AA. hanno richiesto al produttore, tramite investimenti ad-hoc, la realizzazione di plugin per i principali circuiti bancari. Questi plugin sono disponibili, attivi e aggiornati nel tempo e presenti nei sistemi di produzione degli Enti di PP.AA. che attualmente lo utilizzano.

Durante il periodo di valutazione, inoltre, è stato deciso di continuare ad utilizzare questa componente anche sulla base di ulteriori motivi quali:

- una buona molteplicità di Enti a livello nazionale usano questa componente in esercizio, compresi gli Enti partecipanti al progetto PEOPLE LPCE
- per quanto al punto precedente, gli Enti hanno già maturato esperienza nell'utilizzo di questa componente e hanno personale con skill idonei al mantenimento della componente negli ambienti di esercizio

- preservare gli investimenti massimizzando il riutilizzo delle ulteriori estensioni, per l'utilizzo dei diversi circuiti di pagamento, concentrandole a fattor comune rilasciandole in un'unica soluzione

Tra le principali funzioni si evidenziano possibilità di:

1. definizione servizi di pagamento
  - gestione servizi di pagamento
  - gestione servizi esterni di pagamento
  - elenco servizi esterni di pagamento
2. visualizzazione storizzazione pagamenti
  - Storico Contabile
  - Storico Ordini
  - Storico estrazione flussi
3. forzatura Pagamenti
4. forzatura Ordini
5. estrazione flussi

L'architettura funzionale del MIP è descritta in figura seguente.

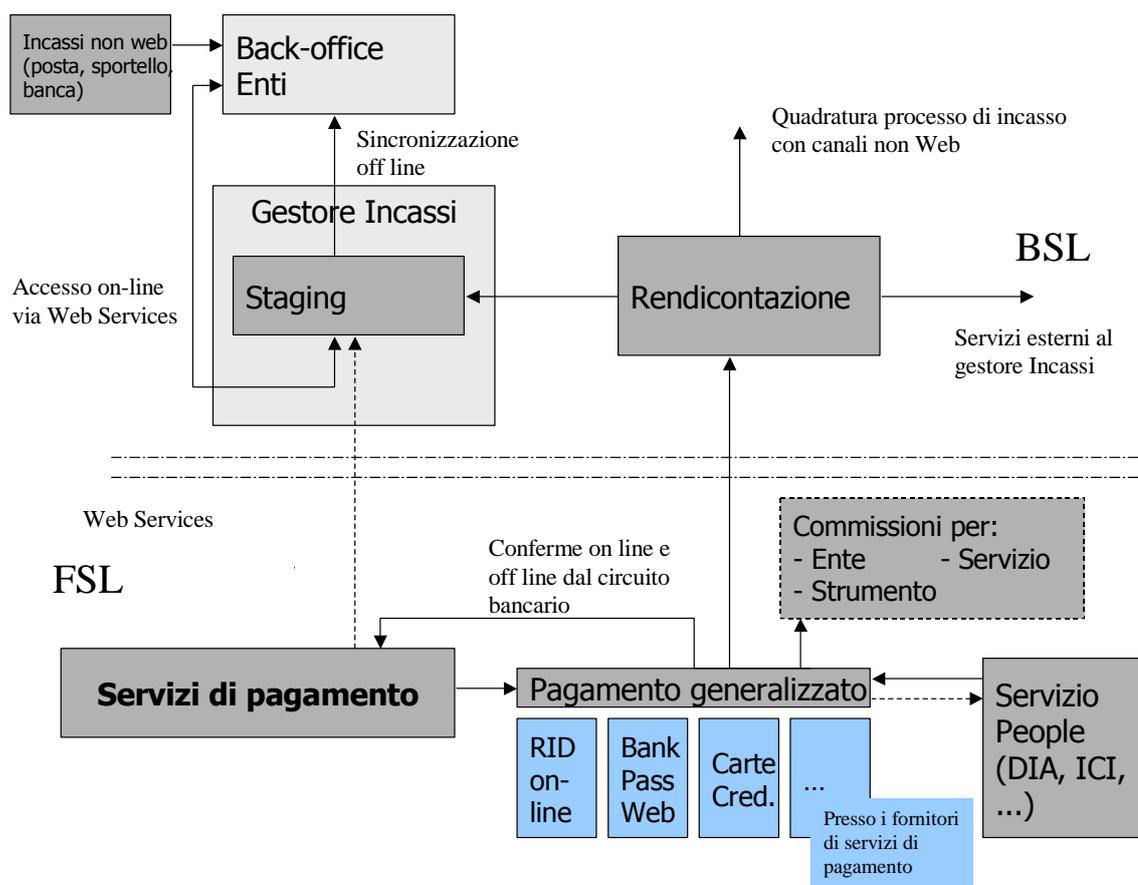


Figura 7

Il MIP soddisfa le richieste dei servizi People che necessitano di far pagare al cittadino somme di danaro.

Periodicamente, a seconda del servizio e dell'ente, vengono realizzati flussi di rendicontazione contenenti i pagamenti effettuati.

Nel pacchetto sono presenti anche i file batch da eseguire periodicamente per:

- la verifica dei pagamenti in sospeso;
- generare i flussi di rendicontazione;
- eseguire le notifiche di pagamento asincrone verso i servizi People che hanno utilizzato il pagamento esterno.

Il protocollo definito tramite applicazione della tecnologia XML permette lo scambio dati tra il MIP ed i server applicativi esterni.

Al fine di facilitare l'integrazione di applicazioni con il Server di Pagamento, sono disponibili alcune librerie per la gestione dei messaggi in accordo con il funzionamento del protocollo XML. Tali librerie, realizzate in tecnologia Java permettono di creare e verificare i messaggi in modo da lasciare all'applicazione il solo compito di gestire i dati applicativi.

Il prodotto è dispiegabile su serverlet-engine freeware Tomcat e utilizza per la gestione delle console di amministrazione pagine jsp.

#### **4.2.3. Plugin integrazione PEOPLE**

Al fine di preservare gli investimenti sostenuti per gli Enti Locali e rendere possibile sia l'erogazione in produzione della soluzione PEOPLE nella versione precedente sia la coesistenza con la soluzione PEOPLE LPCE, sono stati sviluppati due plugin, più comunemente, due forme di integrazione con la gestione dell'identità nella nuova versione LPCE (OpenAM) per le componenti:

1. PEOPLE Framework 2.0.1.L
2. PEOPLE MIP 2.0.1.L

Questi "plugin" consistono in una serie di modifiche al codice sorgente, al fine di assicurare pari funzioni volte ad ottenere la medesima consistenza e comportamento nelle rispettive soluzioni.

Gli ulteriori adattamenti a versioni differenti, non sono incluse nella progettualità della soluzione corrente, viene rilasciato tuttavia il codice sorgente necessario e durante le fasi di trasferimento, saranno restituite le indicazioni tecniche necessarie utili a supportare il ripetersi delle operazioni nelle versioni differenti.

##### **4.2.3.1. Plugin modulo CA-People**

Consiste in modifiche al codice sorgente, apportate alla componente CA-People, la quale si occupa di effettuare il riconoscimento dell'utente, consta di due fasi specifiche; la prima è la protezione a livello di openAM della web application specifica, la seconda è la modifica delle Classi in modo da poter prelevare i dati dell'utente.

Al termine della fase di autenticazione, dopo che OpenAM effettua il riconoscimento dell'utente, la CA-People, preleva le informazioni dell'utente dall'insieme di attributi che costituiscono il profilo dell'utente e le trasferisce fino al livello di front-end dove le informazioni sull'utente vengono estratte ed utilizzate dai vari servizi.

Per quanto riguarda le modifiche del codice della CA-People è necessario introdurre due nuove Classi Java (UserOpenAM.java e Constants.java) che si occupano di recuperare gli attributi e i ruoli dell'utente autenticato con OpenAM.

#### 4.2.3.2. Plugin modulo Pagamenti e incassi (MIP)

L'integrazione di OpenAM con il MIP si compone delle seguenti modifiche alle applicazioni web che gestiscono le Console.

Per la parte riguardante la Mip-console (ovvero il software per la gestione di tutte le specifiche del MIP) si tratta di effettuare le seguenti modifiche:

- introdurre un nuovo parametro nel file ldap\_prof.properties:
  - openam.serviceurl="url specifica della chiama REST di OpenAM (per sempio: <https://identificazione.miosito.it/sso/identity/attributes?subjectid=>
- introdurre un nuovo parametro nel file RglsCIGProfDB.properties:  
ExternalProfilerClass=it.regulus.osa.profile.runtime.extProfiler.OpenAMProfiler
- sostituire la seguente libreria jar profile.jar con la nuova e aggiungere la nuova libreria profile\_openam.jar

Per la parte riguardante la ServerCIGOp (ovvero quella che si preoccupa di gestire l'autenticazione e la profilazione del software Mip Console. Occorre effettuare le seguenti modifiche:

- modifica del web.xml per la valorizzazione dei parametri relativi alla denominazione del cookie e all'indirizzo dove eseguire, durante il ciclo di elaborazione le interazioni REST
 

```
<context-param>
  <param-name>OpenAMCookie</param-name>
  <param-value>iPlanetDirectoryPro</param-value>
</context-param>

<context-param>
  <param-name>OpenAMServiceURL</param-name>
  <param-
value>https://identificazione.miosito.it/sso/identity/attributes?subjectid=<
/param-value>
</context-param>
```
- aggiungere la nuova libreria jar cigserveropenam.jar

#### 4.2.4. Profili utente e sicurezza applicativa

Per esigenze di compatibilità della soluzione PEOPLE, versione precedente e diretta estensione LPCE e di integrazione di sistema (SSO locali e remoti, protocolli di federazione, prodotti terzi), gli utenti e gli operatori del sistema sono registrati nel repository LDAP di OpenLDAP.

E' opportuno ricordare che, nella progettualità della soluzione corrente (LPCE), utenti intesi come cittadini ed operatori formano due classi disgiunte. Inoltre, ciascun operatore è definito in relazione ad uno ed un

solo ente e può operare solo per quello stesso ente. Al contrario, per quanto concerne gli scopi di questo documento, i cittadini non sono associati ad un ente ed hanno libero accesso a tutte le funzioni ad essi dedicate. Questo è il modello proposto nell'ambito della presente soluzione, un modello diverso, tenuto conto dei diversi contesti e delle esigenze è implementabile ma esula dagli scopi della presente progettualità che comunque offre predisposizione per un'implementazione diversa.

#### 4.2.4.1. Struttura della directory utenti

La struttura organizzativa della directory è stata suddivisa in rami funzionali che raggiungono al massimo la profondità di tre livelli. Ogni livello comprende una suddivisione per utenti e per gruppi. In questo modo gli oggetti sono suddivisi funzionalmente per livello e sono raggruppati in gruppi logici. Tutte le entry qui trattate sono raggiungibili dalla radice della directory tramite una query del tipo “cn=<common name>” e non è quindi necessario (né consigliato) l'uso del dn (*distinguished name*) completo. I Rami principali sono così suddivisi per i ruoli amministratori della soluzione, cittadini e operatori:

- cn=amministratori,dc=sp2con-demo,dc=it
- cn=cittadini,dc=sp2con-demo,dc=it
- cn=operatori,dc=sp2con-demo,dc=it

#### 4.2.4.2. Memmorizzazione profili utente OpenLDAP

Agli account creati in LDAP con gli strumenti di gestione previsti corrisponde una entry nel sotto-ramo Users del ramo funzionale di appartenenza, avente come cn (common name) lo username di login dell'account ed appartenente alle seguenti objectClass:

- top
- person
- inetUser
- inetOrgPerson
- organizationalPerson

Il progetto PEOPLE utilizza un diverso profilo per i dati individuali, profilo che è stato ulteriormente esteso nell'ambito del progetto e-Firenze. Per questo motivo, le entry degli account creati per un cittadino appartengono anche alle seguenti objectclass:

- UtentePeople
- UtenteEFirenze

#### 4.2.4.3. Sicurezza applicativa

Una volta avvenuta l'identificazione dell'utente, recuperando dagli attributi del profilo le informazioni di username e gruppo di appartenenza (p.es. CITTADINI, OPERATORE ENTE APPARTENENZA) è possibile utilizzarle come chiave composta per accedere alle tabelle APPLICAZIONI e FUNZIONI APPLICATIVE che descrivono:

- a quali servizi o applicazioni protette l'utente identificato può accedere
- quali funzioni può strumentare nell'ambito del servizio o dell'applicazione protetta

La tabella APPLICAZIONI contiene l'elenco delle applicazioni attive. Le FUNZIONI\_APPLICATIVE sono le particolari funzioni che ciascuna applicazione realizza e che possono essere oggetto di privilegio. E' opportuno ricordare che, nel sistema multi-portale, i privilegi sono esclusivamente associati agli operatori degli enti. Non esistono infatti, per quanto concerne gli scopi di questo documento, differenze di privilegi per i cittadini.

La relazione tra le due (campo ID\_APPLICAZIONE di FUNZIONI APPLICATIVE) è 1:N. Si assume infatti che ciascuna applicazione realizzi almeno una funzione applicativa.

Applicazioni più complesse (e.g. prenotazione risorse) potrebbero realizzare più funzioni applicative (e.g. gestione appuntamenti, visura appuntamenti).

#### 4.2.5. Interfacce di front-end (cittadino)

L'esperienza del Centro Servizi del Comune di Firenze ha evidenziato nel tempo alcuni aspetti fondamentali come l'importanza di preservare l'esperienza dell'utente (user experince) o poterla trasformare in una più innovativa, guardando alla più moderna interazione con le tecnologie Internet del WEB 2.0, oltreché la necessità di poter facilmente realizzare le interfacce utente. Agli aspetti già citati si aggiunge tutta una serie di esigenze derivate dalla comunicazione e di interattività correlata al canale di erogazione, in particolare:

- Deve essere possibile rendere la medesima esperienza utente o costruirne una nuova basata su possibilità di interazione differenti (p.es. web 2.0)
- Le maschere utente di interazione con il front-end devono essere coese, ovvero basate, sugli stessi componenti per ottenere la medesima modalità di interazione
- Deve essere assicurata rapida possibilità di variazione del look and feel
- Deve essere possibile ottenere in modo ripetibile, pari righe di codice sorgente controlli utili a strutturare e comporre nell'insieme le maschere utente
- I controlli devono essere istanziabili con il numero minore di righe di codice per ridurre le possibilità di malfunzionamenti.

Sono stati esaminati tutta una serie di framework per la creazione di controlli e interfacce di front-end. La scelta è ricaduta su Vaadin per:

- maturità di prodotto
- produzione automatica a fronte di una riga scritta nel codice sorgente di tutto il codice corrispondente al tempo di esecuzione: lato server (java) e lato client (javascript)
- controlli certificati standard
- controlli non certificati, estensivi, mantenuti dalla community
- copertura multicanalità (web e mobile)

In modo opzionale assicura, pari codice, astrazione rispetto all'eventuale possibilità di dispiegamento sia come applicazione web standalone, sia all'interno di un contenitore di portale (user integration, basata su applicazioni)

Inoltre, con l'aiuto della rappresentazione della matrice QFD riportata in "Allegato A", possiamo verificare nel dettaglio alcuni precisi aspetti che hanno condotto alla scelta del prodotto Vaadin.

Tale scelta, infatti, risulta giustificata dal possesso di una ricca serie di caratteristiche tecniche che soddisfano la maggior parte dei requisiti, specialmente fra quelli ritenuti più importanti.

Nel dettaglio, Vaadin eccelle nei requisiti tecnici relativi alla **codifica**, garantendo, ad eccezione del governo sulle informazioni di interfaccia utente, la soddisfazione di tutti i requisiti di semplicità di realizzazione e di manutenzione sia del front end che del back end, nonché l'importante aspetto legato alla richiesta di un basso livello di conoscenze tecniche per lo sviluppo.

L'elemento di eccezione, seppur esistente, ha tuttavia il più basso peso relativo fra tutti i requisiti funzionali (Relative weight = 0,5%), tale da rendere inconsistente la differenza di valutazione in termini assoluti tra Vaadin ed i concorrenti (0,00 contro 0,01 e 0,02). Per contro, nell'importante requisito del pieno **supporto nativo per Google App Engine**, Vaadin ottiene un punteggio sensibilmente superiore ai due concorrenti

Mentre per il supporto commerciale i tre prodotti sono valutati tutti ad uno stesso medio livello, Vaadin eccelle insieme a EXTJS per i **temi grafici** e la ricchezza della **documentazione**.

Per quanto riguarda invece la **portabilità** e le **estensioni**, EXTJS è valutato sempre più positivamente, ma, anche in questo caso, gli aspetti non coinvolgono, requisiti di alto livello di importanza.

Complessivamente, aiutati anche dal grafico dei punteggi finali ponderati, possiamo riassumere che il prodotto Vaadin è sempre pari o superiore ai concorrenti per quasi tutti i requisiti tecnici: la valutazione è inferiore solo in corrispondenza di requisiti meno importanti, ragione per cui la differenza con gli altri due prodotti, seppur negativa, è piuttosto contenuta.

Il punteggio finale associato a Vaadin è di 4,45, contro 3,67 di EXTJS e 2,07 di JSR286.

#### 4.2.6. Banche dati

Al fine di favorire l'integrazione di sistemi software con sistemi differenti di banche dati, è stato promosso nell'adozione dello stack tecnologico, un prodotto Object Related Model (ORM).

I prodotti ORM forniscono, mediante un'interfaccia orientata agli oggetti, tutti i servizi inerenti alla persistenza dei dati, astruendo nel contempo le caratteristiche implementative dello specifico database relazionale utilizzato.

I principali vantaggi nell'uso di un tale sistema sono :

- Il superamento (più o meno completo) dell'incompatibilità di fondo tra il software orientato agli oggetti ed il modello relazionale
- Un'elevata portabilità rispetto alla tecnologia utilizzata dai database: cambiando banca dati non devono essere riscritte le routine di controllo e interazione con lo strato di persistenza; generalmente basta cambiare poche righe nella configurazione del prodotto per l'ORM utilizzato.
- Drastica riduzione della quantità di codice da redigere; l'ORM maschera dietro semplici comandi le complesse attività di creazione, lettura, aggiornamento ed eliminazione dei dati (operazioni CRUD). Tali attività occupano di solito una buona percentuale del tempo di stesura, testing e manutenzione complessivo. Inoltre, sono per loro natura molto ripetitive e, dunque, favoriscono la possibilità che vengano commessi errori durante la stesura del codice che le implementa.
- Suggerisce la realizzazione dell'architettura di un sistema software, tendendo pertanto ad isolare in un solo livello la logica di persistenza dei dati, a vantaggio della modularità complessiva del sistema.

Hibernate è stato scelto sulla base della nota maturità. Si tratta di un prodotto licenziato e distribuito in licenza LGPL. Nativamente aggiunge funzionalità per:

- la gestione della concorrenza nell'accesso ai dati, controllando eventuali conflitti durante la modifica di un dato da parte di più utenti in contemporanea
- Meccanismi di caching dei dati. Per esempio, se accade che uno stesso dato venga "letto" più volte dal database, il sistema ORM può fornirlo automaticamente con un supporto di "cache" che migliora le prestazioni e riduce il carico sul sistema di database.

L'uso dello strato software ORM favorisce un miglioramento alla qualità del software, per caratteristiche di manutenibilità e portabilità.

Nell'ambito della soluzione PEOPLE LPCE saranno oggetto dei piani di test, casi per i database di maggior diffusione in soluzioni open e vendor, spesso frequenti negli ambienti di esercizio, meglio specificate MySQL e Oracle. Ulteriori adattamenti a banche dati differenti, esulano dallo scopo della presente soluzione progettuale e saranno oggetto di specifiche attività di configurazione da parte degli Enti partecipanti.

## 5. Trasferimento e manutenzione

---

### 5.1. Codice sorgente

La presente soluzione utilizzerà software FLOSS basati su standard industriali di mercato interoperabili. Il software e la documentazione necessaria prodotta nell'ambito del presente progettualità sarà completa di codice sorgente al fine di rendere possibile il conferimento al Catalogo Nazionale per il riuso della PP.AA..

### 5.2. Licenza di distribuzione

In Italia, l'utilizzo di software Open Source nella Pubblica Amministrazione è in particolare motivato dalle seguenti indicazioni, dove si promuove l'utilizzo di standard aperti e sistemi informatici interoperabili:

- Commissione Europea: Decisione 2004/387/CE: erogazione interoperabile di servizi di governo elettronico alle Pubbliche Amministrazioni, alle imprese e ai cittadini
- Ministero per l'Innovazione e le Tecnologie: Direttiva 19 dicembre 2003: Sviluppo ed utilizzazione dei programmi informatici da parte delle Pubbliche Amministrazioni. In attuazione di tale direttiva, il Centro nazionale per l'informatica nella pubblica amministrazione (DigitPA, ex CNIPA) ha costituito "l'Osservatorio Open Source"

In particolare, DigitPA individua una serie di vantaggi nella distribuzione ed evoluzione del software open source:

- razionalizzazione dei costi
- trasparenza e sicurezza
- non dipendenza da un unico fornitore
- elevata riusabilità
- accessibilità per le piccole realtà di sviluppo

Il software e la documentazione realizzati per il servizio qui descritto saranno consegnati con licenza di tipo "open source" (GPL - General Purpose Licence 1.0 o equivalente). Il tipo di licenza prescelta sarà esplicitamente indicata per le componenti che costituiscono la soluzione e comunque anche in caso di diversità (GPL 1.0 o equivalenti) dovranno permettere il conferimento al Catalogo Nazionale per il riuso e la *ridistribuzione* tra Enti di PP.AA..

### 5.3. Dispiegamento

L'intera piattaforma verrà resa disponibile su macchine virtuali preconfigurate, in modo tale che ciascun utilizzatore possa "accendere" la piattaforma sulla propria infrastruttura ed avere l'ambiente di riferimento funzionante e poter ripetere i test di accettabilità della soluzione. Sono escluse dalla manutenzione correttiva e in genere dalla formazione, tutte le richieste di attività specifiche per l'adattamento parziale o totale dei singoli prodotti che costituiscono la soluzione nei diversi ambienti di riferimento di ogni singolo Ente.

## 5.4. Formazione del personale

Per quanto attiene al dispiegamento, alla necessaria integrazione e adattamento con i sistemi locali, si presuppone che, come prerequisito, siano presenti i seguenti skill pregressi e specifici, descritti tenendo conto dello standard EUCIP (standard europeo per lo sviluppo delle competenze dei professionisti ICT):

### IT Architetto di Sistema

Un progettista di sistemi informatici in grado di assumere un ruolo centrale nella progettazione, integrazione e miglioramento di sistemi IT - con particolare riguardo alle architetture software - curandone anche la sicurezza e le prestazioni; oltre ad una vasta competenza dell'ICT (in tutti i campi: software, hardware e reti) e di tecniche di progettazione specifiche, è richiesta la capacità di descrivere un sistema in termini di componenti, protocolli (HTTPS, SOAP, REST, LDAP, DNS, SAML 2.x) e flussi logici (SSO, applicazioni XML).

### System Integration & Testing Engineer

Un tecnico di collaudo e integrazione di sistemi deve essere efficace in varie aree dello sviluppo di sistemi: preparazione della documentazione per l'utente finale, allestimento di sistemi IT, test delle loro funzioni, sia nel complesso che per singoli moduli componenti, identificazione delle anomalie e diagnosi delle possibili cause. È richiesta anche una conoscenza specifica su come vengono costruite le interfacce tra moduli software e protocolli di rete.

Deve dimostrare una conoscenza comprovata nell'ambito della configurazione e gestione di servizi:

- di identità, Single Sign On e Server LDAP (preferibilmente OpenAM)
- dei Webserver e Middleware: in particolare Apache e Tomcat
- della gestione dei Server DNS e della risoluzione di nomi in generale
- di installazione e configurazione sistemi operativi, con particolare attenzione in ambito Linux, inclusa la conoscenza per la stesura di procedure batch di scripting e manualità nelle configurazioni di base e concetti avanzati

### Software Developer

Un analista programmatore efficace nella realizzazione e manutenzione di moduli software complessi, che tipicamente dovranno essere integrati in un più ampio sistema informativo. Sono possibili diverse specializzazioni, sia nel campo degli applicativi e dei servizi web, sia nel software a livello di sistema. Comprovata esperienza (almeno quinquennale) per:

- Linguaggi di programmazione: Java (incluse le declinazioni web Servlet/JSP) e opzionalmente PHP
- Framework di sviluppo Java preferibilmente Vaadin, Spring, Apache CXF
- Tecnologie: HTML, Javascript, Css
- Realizzazioni applicazioni SOA e protocolli SOAP/REST e XML.
- Databae MySQL, opzionalmente Oracle

Autonomia nell'installazione e gestione delle configurazioni di base delle componenti di Middleware:

- Java JDK/JRE
- Application server Apache, Tomcat

A titolo di collaborazione nel progetto della piattaforma ci si aspetta che i soggetti che saranno coinvolti in modo attivo nelle operazioni di manutenzione in esercizio della soluzione abbiano le stesse competenze.

Alcuni di queste competenze saranno oggetto di un piano di formazione specifico, qualora non già presenti, in quanto il progetto SP2CON non prevede tale tipo di specifica formazione.

Saranno oggetto di un piano di formazione alcune giornate per trasferire le competenze necessarie per le attività di dispiegamento e per la comprensione delle configurazioni e del funzionamento dell'ambiente virtuale di riferimento "as-is" che verrà rilasciato. Le giornate di formazione saranno dedicate a tecnici del Comune di Firenze e a quelli nominati da ANCI. Alle sessioni formative potranno partecipare, in qualità di auditori, eventuali tecnici indicati dai responsabili locali di progetto degli altri Enti partecipanti. E' richiesto tuttavia che i tecnici partecipanti abbiano come prerequisito gli skill tecnici precedentemente citati. In seguito dovrà essere implementata una opportuna attività di formazione per gli utenti (operatori degli Enti).

#### **5.5. Manutenzione correttiva**

Le modalità di manutenzione previste nel presente progetto prevedono che ogni richiesta venga tracciata su una specifica piattaforma di tracking degli errori.

Verranno resi disponibili i download delle nuove versioni e delle eventuali patch intermedie sulle componenti realizzate ad hoc.

La soluzione prevede anche che ci sia un ambiente per la gestione della configurazione e per la storicizzazione dei rilasci del codice sorgente e della documentazione.

## Appendice 1: Le possibili soluzioni

Per poter soddisfare i requisiti meglio sintetizzati ed individuati ai capitoli precedenti, è stata scelta un'architettura di sistema modulare nella quale ogni modulo assolve ad una specifica funzione.

Stante la necessità di corretta interoperabilità tra i moduli, è stata effettuata sia una verifica sulle specifiche dichiarate sia dei test che circa l'effettivo funzionamento nello specifico contesto.

Il mondo Open Source offre una molteplicità di soluzioni per assolvere alle funzioni analizzate precedentemente.

L'ambito operativo di questa sezione riguarda la verifica di ogni singola componente e il relativo interfacciamento tra ogni modulo al fine di realizzare una soluzione completa.

Emergono subito vincoli legati a tali interfacciamenti: spesso l'integrazione tra le varie componenti risulta operativamente sconveniente e richiede l'ausilio di workaround che rendono la soluzione potenzialmente instabile nel suo complesso.

A tal fine sono state individuate tre tipologie di sviluppo, in base ai prodotti analizzati.

Inoltre le soluzioni qui presentate constano di tutte le componenti relative alla gestione ed alla memorizzazione degli utenti, così come le componenti relative alla gestione del modulo dei pagamenti e della componente People Light.

Le soluzioni, grazie alla modularità che le caratterizzano, risultano **autoconenute** ma **opzionalmente** possono essere integrate con ambienti di presentazione delle informazioni, quali, content management system (CMS) e portali.

Per soluzioni autoconenute si intende il rispetto e l'esecuzione di tutte le funzioni citate senza obbligo di utilizzare altri moduli di presentazione.

E' riportato di seguito lo schema a blocchi di tre stack tecnologici possibili per realizzare la soluzione sulla base di quanto finora descritto.

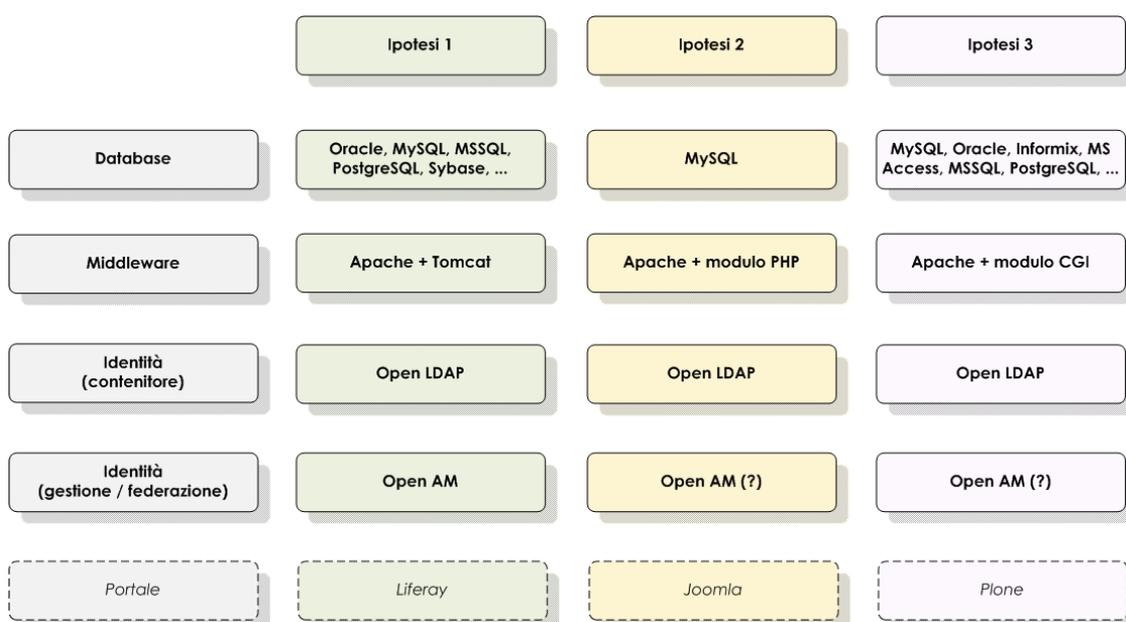


Figura 8

Per individuare le possibili soluzioni è stato utilizzato il metodo del Quality Function Deployment (QFD); tale strumento ha aiutato nell'identificazione e strutturazione dei bisogni e nella loro traduzione in caratteristiche quantitative misurabili.

L'attività svolta è stata, quindi, suddivisa nelle seguenti quattro fasi:

1. reperire, prioritizzare e pesare le esigenze del cliente (i bisogni)
2. individuare le caratteristiche tecniche del prodotto
3. creare la matrice delle relazioni fra caratteristiche e bisogni
4. effettuare un benchmarking con i "best in class" e pianificare le linee di sviluppo del futuro prodotto

In particolare i requisiti utente individuati sono stati i seguenti:

- Sicurezza applicativa finale
- Semplicità realizzazione front-end
- Semplicità realizzazione back-office
- Semplicità manutenzione front-end
- Semplicità manutenzione back-office
- Conformità ai criteri di accessibilità
- Migrabilità su altri prodotti
- Adattabilità alla multicanalità
- Maturità della tecnologia
- Immagine coordinata

Ed i requisiti funzionali individuati sono stati i seguenti:

- Vasta compatibilità browser (nativa)
- Plugin browser non richiesti
- Monocodifica dei sorgenti
- Automatizzazione controlli interfaccia utente (nativa)
- Dispiegabilità automatica in forma portlet (nativa)
- Programmazione Javascript non richiesta
- Conoscenza HTML non necessaria
- Governo sulle informazioni di interfaccia utente
- Portabilità del codice su altri prodotti (es. content management system e portali)
- Portabilità del codice su altri canali (p.es. supporto nativo per mobile e Google App Engine)
- Estensione Add-on / Componenti complessi per la realizzazione di interfacce
- Temi grafici
- Documentazione
- Supporto commerciale

Si riporta in Allegato A la matrice QFD dell'analisi effettuata. Le soluzioni esaminate ed individuate verranno descritte nel prosieguo del presente capitolo e del successivo.

Rispettando la specifica di utilizzo di software FLOSS, sono state esaminate le soluzioni maggiormente diffuse (e supportate) per ognuno dei seguenti ambiti:

## Gestione e federazione delle identità, Single Sign On

Questo componente permette di autenticare gli utenti esterni una sola volta, dopodiché questi possono accedere a tutte le aree cui hanno diritto senza la necessità di dover reimmettere le credenziali

### Contenitore delle identità

Questo componente è il vero e proprio archivio delle credenziali e dei diritti di tutti gli utenti del sistema

### Middleware

Il middleware scelto per lo sviluppo si basa su Java. Tale scelta è dettata dal fatto che la maggior parte dei prodotti FLOSS è dispiegabile in ambienti tomcat che si basano sulla tecnologia Java. Altre tecnologie disponibili per il supporto middleware si basano su script php o script python o ancora perl. La scelta è ricaduta su Java perchè, al netto delle risorse necessarie, gli applicativi Java vantano performances ottimali, e supportano nativamente le strutture di thread e sincronizzazione. Tali funzioni sono molto limitate negli altri framework disponibili per ambienti FLOSS.

## 1.1. Modulo gestione e federazione delle identità

**Shibboleth:** è un framework open source basato su SAML implementato da Internet2. Tramite Shibboleth si può realizzare il Single Sign On istituzionale autenticando gli utenti localmente e autorizzandoli ad accedere alle risorse in base ad informazioni scambiate dalle organizzazioni in modo sicuro.

- Mancanza di ulteriori standard e possibilità di adattamento “nativo” per l’integrazione basata su standard con altri prodotti.
- Necessità di una componente ulteriore per il funzionamento in modalità CAS.
- Impossibilità di recuperare il profilo dell’utente completo tramite unica interazione ad una componente specifica; occorre doppia interazione incluso il sistema LDAP.
- Impossibilità di collocare il server LDAP al terzo livello di rete (e sicurezza) dedicato esclusivamente alla gestione dei dati.
- Il server LDAP in questo caso rimarrebbe collocato a livello di middleware (secondo livello di rete).

**JOSSO:** è distribuito in due versioni, quella Enterprise e quella OpenSource.

La versione OpenSource risulta essere limitata in quanto:

- non supporta target host remoti basati su Apache Tomcat
- non supporta nativamente lo standard SAML2
- non consente di essere installata in modalità cluster, quindi limita notevolmente le possibilità di espansione
- il supporto ai Database utenti non è garantito nella versione OpenSource, per tanto, tale software riduce le scelte degli applicativi di backend e rende le configurazioni molto più vincolate a prodotti, venendo meno al prerequisito di modularità

**CoSign:** è un prodotto molto limitato in quanto consente di proteggere le sole risorse Apache:

- non supporta lo standard SAML
- le fasi di sviluppo risultano essere estremamente lente
- non beneficia di un supporto adeguato
- l'installazione risulta avere molti problemi con i sistemi a 64 bit, richiedendo svariati workaround che potrebbero rendere il prodotto instabile e limitano la portabilità e l'estendibilità della soluzione.

**OpenAM:** sviluppato dall'azienda ForgeRock, la quale è stata insignita del titolo "Cool Vendors in Identity Management" da parte di Gartner.

Si rilevano le seguenti caratteristiche distintive:

- Capacità di integrazione (REST, Web Service, API)
- Elevate performances dichiarate, anche grazie alla possibilità di installare il framework in modalità cluster
- Personalizzazione Plugin modalità di autenticazione
- Aderenza allo standard SAML2
- Semplicità di estensione remota delle funzioni di SSO tramite installazione plugin
- Integrazione nativa motore di portale Liferay
- Supporto enterprise da parte della stessa casa sviluppatrice
- Supporto esteso ad una grande molteplicità di Database utenti

## 1.2. Modulo contenitore delle identità

I sistemi oggetto di comparazione sono stati: Open Ldap, Apache Directory, Open DS, 389 Directory Server.

Active directory e Novell eDirectory sono stati esclusi dalla comparazione in quanto non Open Source.

### Open Ldap:

- Prodotto largamente diffuso
- Ampiamente aderente agli standard
- Le funzionalità non sono limitate e vanno oltre a quelle previste dai prodotti CAS
- Performance dichiarate: oltre cinque milioni di oggetti con risposte al di sotto del secondo
- Supportato dalla comunità. Maggiore disponibilità di documentazione
- E' utilizzato dalle più importanti aziende di tipo enterprise e università mondiali, con riscontri favorevoli
- Sicurezza: restituisce il profilo dell'identità in modo completo senza necessità di accessi diretti al contenitore
- Supera il problema della memorizzazione del certificato
- Supera i problemi di sicurezza legati ai nuovi standard previsti dai più recenti browser

### Apache Directory:

- Server compatibile LDAP v3
- Interamente scritto in Java
- Licenza AFS (Apache Software Foundation)

- Utilizzabile in modalità integrata o come demone
- Supporto Kerberos 5

#### Open DS:

- Interamente scritto in Java
- Implementa un ampio range di standard LDAP, tra LDAP v3 e DSMLv2
- Replica multi master
- Controllo degli accessi via ACL
- Rilasciato sotto licenza Sun Microsystems's Common Development and Distribution (CDDL)

#### 389 Directory Server:

- Replica Multi-Master fino a 4 nodi
- Supporto per i protocolli SSLv3, TLSv1 e SASL, LDAP v3
- Codice sviluppato da 10 anni (389ds discende da RedHat DS, che a sua volta viene da Netscape DS)
- Documentazione completa (riferimento RedHat DS)
- Controllo degli accessi via ACL

La scelta è ricaduta su OpenLDAP sia per motivi legati al know how interno, sia perché è stata valutata con favore la maturità e la grande diffusione del progetto poiché garantiscono un vasto supporto alla soluzione.

In virtù della modularità della soluzione, il contenitore delle identità può comunque essere scelto arbitrariamente. E' tuttavia sottointeso che la struttura degli schemi e l'organizzazione delle informazioni in genere, affinché sia garantito il corretto funzionamento della soluzione, senza ulteriori personalizzazioni, dovrà essere mantenuta pari forma.

### 1.3. Funzioni del sistema

**Gestione delle credenziali e dei profili degli utenti:** Le credenziali ed i profili saranno gestiti da un componente centrale di Identity and Access Management compatibile con gli standard LDAP3 e SAML2; tale sistema sarà inoltre conforme alla normativa nazionale ed al C.A.D.

Tale sistema si occuperà del recupero dei profili degli utenti così da garantire la centralità del profilo stesso.

Sarà possibile effettuare accesso in lettura alle informazioni tramite le tecnologie: Web Service, REST, API.

**Supporto di tecnologie software differenti:** Saranno supportati i middle tier Tomcat ed Apache ed i linguaggi di programmazione php, java (struts, spring, jsf, vaadin, wicket).

**Gestione dei fault applicativi:** L'architettura completamente modulare adottata garantisce che in caso di fault applicativo di una delle componenti dell'architettura, sia ridotto l'impatto ad un gruppo di componenti ristretto, senza inficiare il funzionamento generale del sistema.

**L'ambiente di virtualizzazione** che costituisce pre-requisito (e rimane non incluso nella soluzione), aggiunge una serie di funzionalità specifiche in tema di

alta affidabilità e bilanciamento dei carichi di elaborazione. Nei paragrafi seguenti, sono riportate alcune informazioni di approfondimento.

**Erogazione in modalità multicanale:** I servizi della piattaforma saranno disponibili via web, mobile, piattaforme social e google apps

**Supporto dei database:** La struttura applicativa sarà in grado, con adattamenti alle configurazioni, di colloquiare con i database Oracle e MySQL.

**Staticizzazione dei contenuti:** Il sistema permetterà di staticizzare i contenuti di pagina determinando una precisa URL di riferimento per l'erogazione dei servizi e dei contenuti informativi.

**Reportistica e statistica:** Tutti i componenti qui descritti devono essere predisposti per l'interazione con il sistema multiportale per le funzioni di business intelligence.

In particolare, ciascun componente deve essere in grado di esportare periodicamente i dati completi di utilizzo in specifiche tabelle del database aventi un formato concordato

#### 1.4. La piattaforma di sistema

Al fine di soddisfare i requisiti di alta affidabilità richiesti dalla soluzione è necessario disporre come pre-requisito di un ambiente virtualizzato che possa garantire i seguenti benefici e funzionalità:

- Alta affidabilità: è infatti possibile installare più server fisici all'interno del datacenter, sui quali dispiegare la soluzione; tali server potranno fungere uno di backup all'altro in caso di guasto o malfunzionamento
- Elevate prestazioni: grazie alla possibilità di allocare, anche dinamicamente, le macchine virtuali su più piattaforme hardware è possibile gestire i picchi di richieste, senza blocchi né rallentamenti del sistema e senza la necessità di acquisire nuove macchine
- Clusterizzazione nativa dei sistemi: grazie alla possibilità di spostare le macchine virtuali, anche in funzione (senza compromettere l'erogazione dei servizi), tra server fisici, viene garantito il funzionamento dei servizi anche in caso di guasto di un server
- Portabilità della piattaforma software: la soluzione permette la creazione di server virtuali hardware independent e contenuti all'interno di un file, così da rendere assai semplice il trasferimento di un sistema da un datacenter ad un altro, ovvero sia la distribuzione dell'intera piattaforma PEOPLE LPCE in un formato standard, indipendente dall'hardware, che non richiede re installazioni di sistema e subito funzionante nel nuovo datacenter

Il sistema operativo prescelto è Linux Debian, distribuito sotto licenza GPL. È stata fatta la scelta di avere un unico sistema operativo (benché installato su una molteplicità di server virtuali) a beneficio della semplicità, gestibilità e manutenibilità del progetto. La versione del sistema operativo sarà l'ultima stable disponibile alla data di rilascio del progetto, al fine di massimizzare la vita utile durante la quale sono rilasciati gli aggiornamenti e le patch di sicurezza.

## 1.5. La sicurezza

La focalizzazione sulla sicurezza è una caratteristica trasversale all'intero progetto. La continuità di servizio, aspetto basilare della sicurezza, è stata garantita dalle scelte pocanzi descritte e dalla modularità con cui il software è stato progettato e verrà realizzato. L'integrità e la confidenzialità dei dati sarà affidata sia a metodologie di scrittura del codice realizzato sia all'architettura di sistema e alle politiche di gestione di seguito descritte.

L'architettura di riferimento prevede la compartimentazione dei sistemi in tre distinte aree di sicurezza (cfr. **Errore. L'origine riferimento non è stata trovata.**) al fine di massimizzare la protezione dei dati, che risiederanno nei database ed LDAP server, ovvero nello strato più interno dell'architettura.

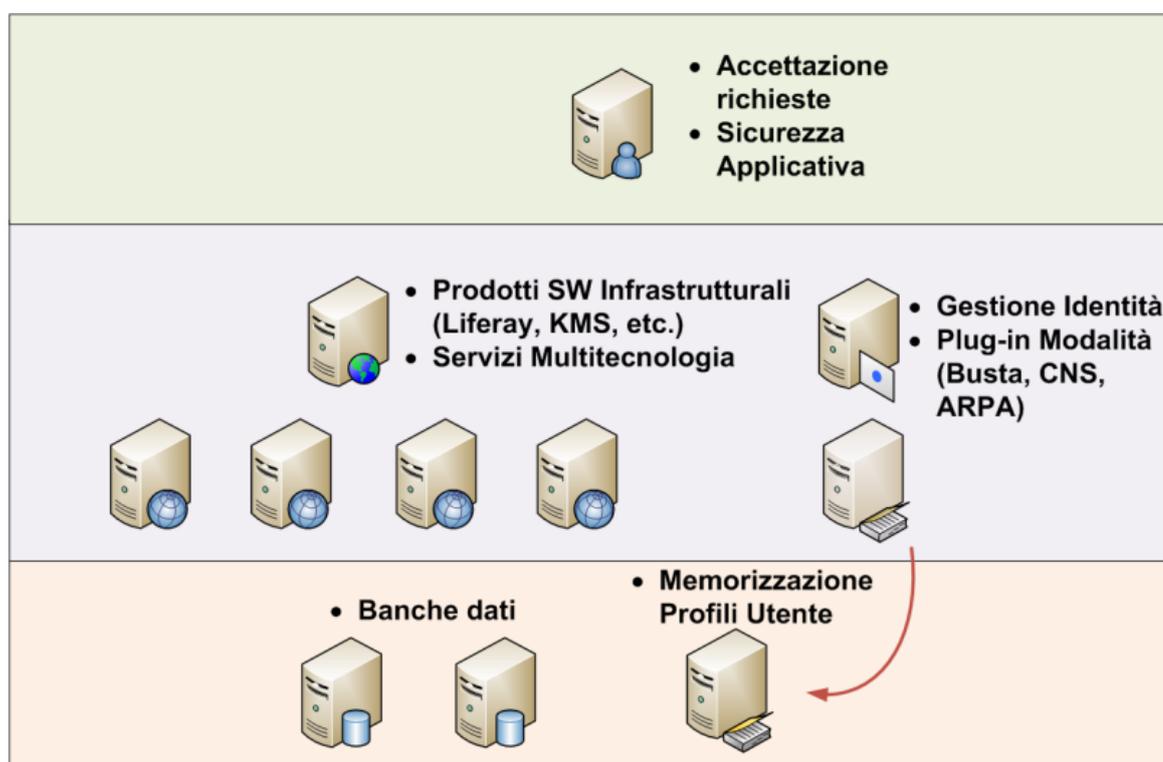


Figura 9

Ogni livello di firewall implementerà politiche restrittive, ovvero saranno consentiti esclusivamente i flussi dati necessari all'erogazione del servizio.

Tutti gli scambi dati LDAP della componente di gestione delle identità avverranno esclusivamente sul protocollo cifrato LDAPS, anche nel core del datacenter.

Gli interfacciamenti tra i diversi moduli del sistema PEOPLE LPCE avverranno previa autenticazione ed i diritti di tali utenti seguiranno il principio di non concedere il permesso di scrittura se non nei casi espressamente previsti.

Tutti i server installati sui server saranno scelti alla più recente versione rilasciata per la distribuzione del sistema operativo, in modo tale che siano ricompresi tutti gli aggiornamenti di sicurezza.

Verranno implementati meccanismi di user lockout, ovvero dopo 15 tentativi errati di autenticazione, l'attività dell'utente viene bloccata per 1 ora.

Tutti i sistemi saranno oggetto di backup notturno.

## 1.6. Valutazione delle soluzioni individuate

Nella valutazione delle soluzioni individuate sono stati presi in considerazione diversi aspetti, anche sulla base dei seguenti fattori:

- Esperienze pregresse del Centro Servizi del Comune di Firenze
- Competenze e formazione del Nazionale del Riuso
- Caratteristiche tecniche dei prodotti e rispondenza ai requisiti funzionali richiesti:
  - Possibilità di inserire applicazioni eterogenee all'interno di un unico ambiente omogeneo e richiedendo un unico login all'utente
  - Supporto di tutti gli standard più importanti e diffusi
  - Supporto di livello enterprise erogato direttamente dalla casa madre
  - Linguaggio di programmazione Java (know how elevato da parte di Linea Comune)
  - Ampia diffusione ed accettazione (anche all'interno della Pubblica Amministrazione)

I portali Joomla e Plone invece hanno dimostrato una bassa attitudine alla possibilità di servire, tramite un unico ambiente, applicazioni eterogenee in ambiente di Single Sign On, rivelandosi adatti ad un uso di CMS ma non di portale. Ciononostante è possibile utilizzare sia Joomla che Plone, purché vengano effettuate molte customizzazioni, a detrimento della manutenibilità e futura possibilità di aggiornamento.

All'analisi sulla sicurezza è risultato che Joomla, in tutta la sua storia, è stato frequentemente gravato da difetti che permettevano un uso improprio del prodotto.

Per il prodotto Plone va segnalato che il linguaggio di programmazione utilizzato (Python) ha una scarsa diffusione e, pertanto, potrebbe essere più difficile in futuro trovare esperti in grado di effettuare manutenzione e customizzazioni, con probabili aggravii economici per gli Enti utilizzatori.

Per il prodotto Joomla va segnalato che non risulta interoperabile con il database Oracle, il che comporterebbe mancanza di retro compatibilità con il precedente progetto PEOPLE e con le basi dati di molti Enti.

## Appendice 2: Prove sperimentali

---

Stanti le componenti di servizio e le possibili architetture di insieme individuate, sono state effettuate delle prove sperimentali con i seguenti scopi:

- Valutare l'integrabilità ed interoperabilità delle diverse componenti
- Valutare le performances
- Valutare la rispondenza delle specifiche dichiarate al contesto di utilizzo

Ripristinare i sistemi a seguito di eventi distruttivi

### 1.1. Configurazioni

Di seguito vengono descritte le configurazioni dei sistemi oggetto delle prove sperimentali.

Gli **application server** sono stati realizzati su server Apache HTTP Server vers. 2.2, Java VM 1.6 ed Apache Tomcat 6, installati su Sistema Operativo Debian 6.0.

Il server di **front end** dell'**Identity Management** è stato realizzato su server OpenAM vers. 9.4, installato su Sistema Operativo Debian 6.0. E' stato effettuato un tuning delle configurazioni per aumentare le prestazioni nel contesto di utilizzo. Il servizio è stato reso accessibile solo il HTTPS. Al fine di offrire una maggiore granularità e protezione, sono stati configurati diversi realm in modo da poter combinare diversi livelli sullo schema LDAP, così da poter offrire più livelli di autenticazione, es. CNS, user input o entrambe. Il repository dei dati è stato appoggiato ad un distinto server LDAP, in rispetto del principio progettuale della modularità, compartimentazione e sicurezza. L'interfacciamento con il server LDAP di back end avviene esclusivamente tramite protocollo cifrato LDAPS e con diritti di sola lettura.

Il server di **back end** dell'**Identity Management** è stato realizzato su server OpenLDAP vers. 2.4, installato su Sistema Operativo Debian 6.0.

Il **database server** di back end è stato realizzato su server MySQL vers. 5.1, installato su Sistema Operativo Debian 6.0.

Lo schema LDAP è stato ramificato secondo le necessità in base all'esperienza dei progettisti, riuscendo a mantenere un numero di livelli non superiore a 3, andando a diversificare i ruoli: degli utenti amministratori, operatori e cittadini (ruolo a sua volta diviso tra credenziali forti e deboli).

È stato effettuato un tuning del server LDAP, è stata aumentata l'indicizzazione degli elementi della directory ed è stata aumentata la cache degli oggetti.

Tutti i server hanno l'orologio di sistema sincronizzato, al fine di garantire la correttezza dei dati delle transazioni e poter garantire un maggior valore ad eventuali analisi dei log.

## 1.2. Modalità di esecuzione delle prove

Sono state effettuate delle prove sperimentali sia al fine di individuare le configurazioni più idonee e performanti sia per misurare i limiti del corretto funzionamento in funzione del carico.

Di seguito verranno riportati i risultati dei test condotti sui due principali componenti del sistema: il server web di front end, e l'application server PEOPLE LPCE (soluzione dispegata); verranno inoltre richiamati i risultati derivanti dall'ottimizzazione del database LDAP.

Per l'esecuzione dei test di performance è stato utilizzato l'applicativo Apache JMeter; frutto di un progetto open source e destinato principalmente al test di carico e funzionale delle applicazioni di tipo web; grazie ai numerosi plugin, connettori e script disponibili, tale sistema risulta anche un ottimo strumento per il test di database, server di posta, server Java Enterprise (JEE), LDAP. Tale applicativo permette di simulare la concorrenza attraverso i threads, permettendo quindi di misurare la performance al variare del carico attraverso la generazione di valori statistici come la media, la mediana, la varianza ed il throughput.

## 1.3. Risultati emersi

Di seguito si riportano i risultati, relativi al web server Apache di front end, nelle seguenti condizioni:

1. Apache configurato in modalità prefork e sottoposto a 250 richieste contemporanee. (Cfr. **Errore. L'origine riferimento non è stata trovata.**Errore. L'origine riferimento non è stata trovata.Figura 10**Errore. L'origine riferimento non è stata trovata.**)
2. Apache configurato in modalità prefork e sottoposto a 1000 richieste contemporanee.
3. Apache configurato in modalità worker e sottoposto a 250 richieste contemporanee.
4. Apache configurato in modalità worker e sottoposto a 1000 richieste contemporanee.

Modalità	Richieste contemporanee	Errore %	Throughput
Prefork	250	0%	3,4/sec
Prefork	1000	92,60%	10,6/sec
Worker	250	0%	25,2/sec
Worker	1000	0%	384,6/sec

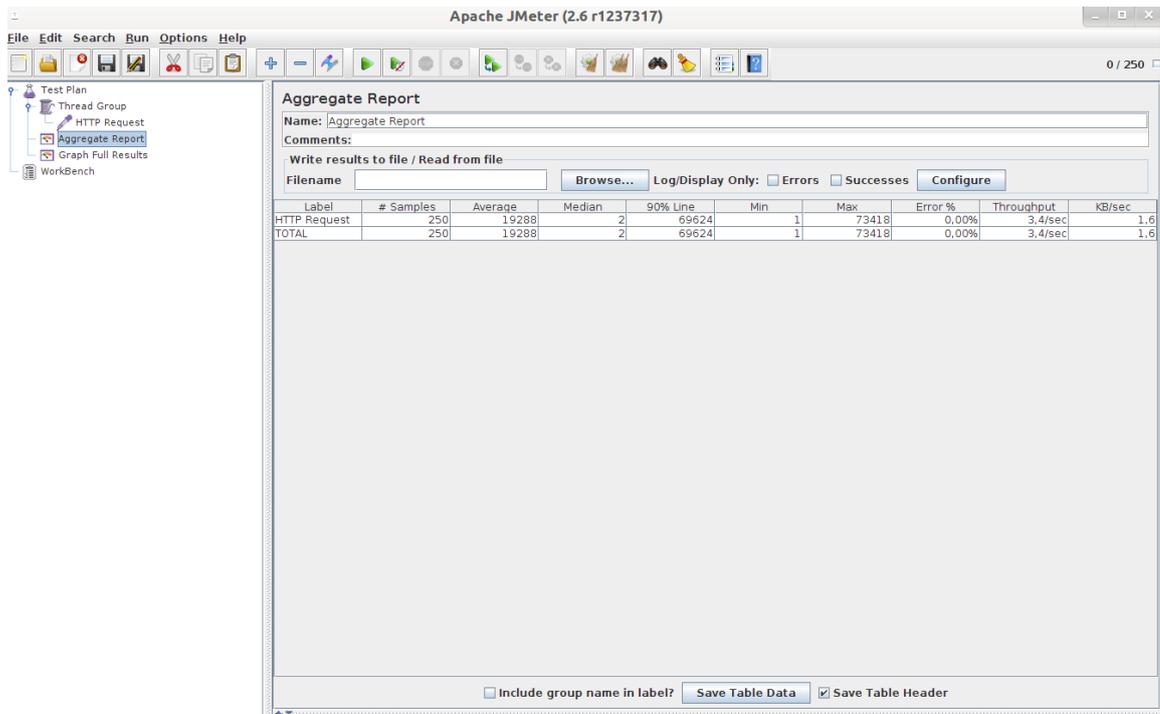


Figura 10

Come si può vedere dai risultati dei test, la scelta di utilizzare il modulo worker al posto del prefork porta ad un incremento prestazione di un fattore oltre 7 nel caso di 250 richieste contemporanee, mentre nel caso di 1000 richieste il fattore di miglioramento è oltre 36 volte e, soprattutto, la percentuale di eccezioni nelle risposte rimane pari allo 0%.

Per quanto riguarda i test di performances sul sistema LDAP, si rileva che per l'estrazione di 20.000 oggetti, il tempo impiegato in assenza di ottimizzazioni risultava variabile in un range dai 3 ai 5 minuti, mentre dopo le ottimizzazioni esso risulta stabilmente nel range 300-400 millisecondi.

Infine, sono stati effettuati stress test sull'application server di PEOPLE LPCE nelle seguenti condizioni:

- 40 richieste contemporanee (cfr. risultati in Figura 11)
- 100 richieste contemporanee
- 200 richieste contemporanee
- 400 richieste contemporanee
- 935 richieste contemporanee

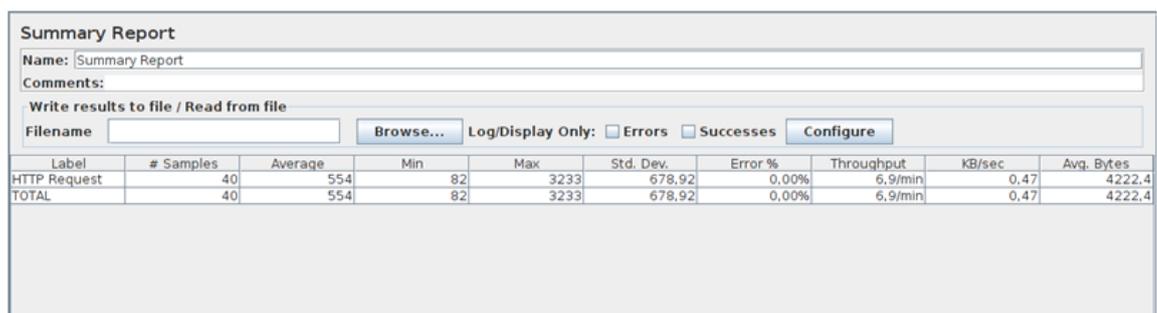


Figura 11

<b>Richieste contemporanee</b>	<b>Errore %</b>	<b>Throughput</b>
40	0%	6,9/min
100	0%	17,2/min
200	0%	33,7/min
400	0%	1,1/sec
935	8,98%	1,7/sec

Come si può evincere dai test sopra riportati, l'application server PEOPLE LPCE mostra una crescita lineare nelle prestazioni di risposta alle richieste fino al limite delle circa 900 richieste contemporanee i cui l'attuale dimensionamento del sistema di test è al limite.

---

## Appendice 3: Quadro normativo

---

Il nuovo CAD, il Codice dell'Amministrazione Digitale (Decreto legislativo n. 235/2010) rinnova il quadro normativo in materia di amministrazione digitale definito nel 2005 con il Decreto legislativo n. 82. Il nuovo CAD introduce un insieme di innovazioni normative che incidono concretamente sui comportamenti e sulle prassi delle amministrazioni e sulla qualità dei servizi resi. La riforma rende così effettivi i diritti per cittadini e imprese, cogenti gli obblighi per la PA, dà sicurezza agli operatori circa la validità, anche giuridica, dell'amministrazione digitale.

Alcuni dei principali cambiamenti introdotti dalla riforma del CAD sono di seguito sintetizzati:

- Validità dei documenti informatici (art. 22, 23, 23-bis, 23-ter): il nuovo CAD fornisce indicazioni sulla validità delle copie informatiche di documenti con riferimento preciso circa le diverse possibilità (copia digitale del documento cartaceo, duplicazione digitale, ecc.)
- Conservazione digitale dei documenti (artt. 43-44 bis): è prevista la gestione della conservazione dei documenti e del relativo processo da parte di un Responsabile della conservazione che si può avvalere di soggetti pubblici o privati che offrono idonee garanzie
- Posta elettronica certificata (artt. 6 e 65): la PEC diventa il mezzo più veloce, sicuro e valido per comunicare con le PA. I cittadini possono utilizzare la PEC anche come strumento di identificazione, evitando l'uso della firma digitale
- Siti pubblici e trasparenza (art. 54): il nuovo CAD arricchisce il contenuto dei siti istituzionali delle amministrazioni, prevedendo che sugli stessi siano pubblicati, in modo integrale, anche tutti i bandi di concorso. La norma obbliga le PA ad aggiornare i dati e le notizie che per legge devono essere pubblicati sul proprio sito istituzionale. Anche tale aspetto viene considerato ai fini della valutazione dei dirigenti
- Customer satisfaction dei cittadini su Internet (artt. 54 e 63): le PA sono tenute ad adottare strumenti idonei alla rilevazione immediata, continua e sicura del giudizio dei propri "clienti" sui servizi online
- Moduli on line (art. 57): le PA hanno l'obbligo di pubblicare online l'elenco dei documenti richiesti per procedimento (moduli e formulari validi) e non possono richiedere l'uso di moduli o formulari che non siano stati pubblicati sul web. La mancata pubblicazione è rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti responsabili
- Trasmissione delle informazioni via web (art. 58): le PA non possono richiedere informazioni di cui già dispongono
- Comunicazioni tra imprese e amministrazioni (art. 5 bis): la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti (anche a fini statistici) tra imprese e PA (e viceversa) avviene solo utilizzando tecnologie ICT
- Accesso ai servizi in rete (artt. 64 e 65): per l'accesso ai servizi erogati in rete dalle Pubbliche Amministrazioni è possibile utilizzare strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, previa individuazione del soggetto che ne richiede il servizio

- Firme (artt. 1, comma 1, lett. q-bis, e 28, comma 3-bis): viene introdotto il concetto di firma elettronica avanzata, con cui è possibile sottoscrivere un documento informatico con piena validità legale
- Carta di identità elettronica e Carta nazionale dei servizi (art. 64): Carte di identità elettronica e Carte nazionale dei servizi valgono ai fini dell'identificazione elettronica
- Pagamenti elettronici (art. 5): il nuovo CAD introduce alcuni strumenti (carte di credito, di debito o prepagate e ogni altro strumento di pagamento elettronico disponibile) per consentire alle PA di riscuotere i pagamenti. Inoltre, permette loro di avvalersi di soggetti anche privati per la riscossione
- Protocollo informatico, fascicolo elettronico e tracciabilità (artt. 40-bis e 41): è previsto che ogni comunicazione inviata tramite PEC tra le PA e tra queste e i cittadini o le imprese sia protocollata in via informatica. L'amministrazione titolare del procedimento raccoglierà gli atti, i documenti e i dati del procedimento medesimo in un fascicolo elettronico, dotato di un apposito identificativo
- Open data (artt. 52 e 68): il nuovo CAD mette in primo piano la responsabilità delle PA nell'aggiornare, divulgare e permettere la valorizzazione dei dati pubblici secondo principi di open Government

la Legge n. 106 del 12 luglio 2011 (di conversione del Decreto Legge n. 70 del 13 maggio 2011, il c.d. "Decreto sviluppo") all'art. 6 impone alle PA l'obbligo di pubblicare sui propri siti istituzionali, per ciascuna procedura, l'elenco degli adempimenti e la documentazione necessaria. In caso di inadempienza, la PA non può rifiutare l'istanza del cittadino o dell'impresa e può solo richiedere l'integrazione della documentazione.

La Legge 9 gennaio 2004, n. 4 (ed i successivi regolamenti attuativi) ha stabilito le norme di accessibilità degli "strumenti informatici" in favore dei soggetti disabili, ovvero ha introdotto l'obbligo per le pubbliche amministrazioni di dotarsi di siti web accessibili.

La regolamentazione in materia di privacy è definita dal Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (c.d. Codice della Privacy), in vigore dal 1 gennaio 2004 che, in materia informatica, prevede il rispetto di misure minime di sicurezza ed introduce specifici adempimenti. Le prescrizioni contenute nel Codice della Privacy sono state, successivamente, aggiornate dai seguenti provvedimenti normativi:

- Decreto legislativo 28 maggio 2012, n. 69
- Decreto Legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla Legge 4 aprile 2012, n. 35
- Decreto Legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla Legge 22 dicembre 2011, n. 214;
- Decreto Legge 13 maggio 2011, n. 70 convertito, con modificazioni, dalla Legge 12 luglio 2011, n. 106
- Legge 4 novembre 2010, n. 183;
- Legge 29 luglio 2010, n. 120
- Decreto-Legge del 25 settembre 2009, n. 135 convertito, con modificazioni, dalla Legge 20 novembre 2009, n. 166
- Legge 4 marzo 2009, n. 15

- Decreto-Legge del 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla Legge 27 febbraio 2009, n. 14
- Decreto-Legge 25 giugno 2008, n. 112 convertito, con modificazioni, dalla Legge 6 agosto 2008 n. 133
- Decreto legislativo 30 maggio 2008, n. 109
- Legge 18 marzo 2008, n. 48, ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
- Decreto-Legge 28 dicembre 2006, n. 300 convertito, con modificazioni, dalla Legge 26 febbraio 2007, n. 17
- Decreto-Legge 12 maggio 2006, n. 173 convertito, con modificazioni, dalla Legge 12 luglio 2006 n. 228
- Decreto-Legge 30 dicembre 2005, n. 273 convertito, con modificazioni, dalla Legge 23 febbraio 2006, n. 51
- Decreto Legge 30 novembre 2005, n. 245 convertito, con modificazioni, dalla Legge 27 gennaio 2006, n. 21
- Decreto legislativo 7 settembre 2005, n. 209
- Decreto-Legge 27 luglio 2005, n. 144 convertito, con modificazioni, dalla Legge 31 luglio 2005, n. 155
- Decreto-Legge 30 dicembre 2004, n. 314 convertito, con modificazioni, dalla Legge 1 marzo 2005, n. 26
- Decreto-Legge 9 novembre 2004, n. 66 convertito, con modificazioni, dalla Legge 27 dicembre 2004, n. 306
- Decreto-Legge 24 giugno 2004, n. 158 convertito, con modificazioni, dalla Legge 27 luglio 2004, n. 188
- Decreto-Legge 29 marzo 2004, n. 81 convertito, con modificazioni, dalla Legge 26 maggio 2004, n. 138
- Decreto legislativo 22 gennaio 2004, n. 42
- Decreto-Legge 24 dicembre 2003, n. 354 convertito, con modificazioni, dalla Legge 26 febbraio 2004, n. 45

Vi sono poi le Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato anche da soggetti pubblici per finalità di pubblicazione e diffusione sul web (Deliberazione 2 marzo 2011), che forniscono una serie di misure ed accorgimenti a cui le amministrazioni si devono attenere quando comunicano o diffondono, tramite il proprio sito istituzionale, dati personali, quando fanno pubblicità all'azione amministrativa, quando permettono la consultazione di atti. In modo particolare tali Linee guida affrontano gli aspetti legati alla correttezza e all'aggiornamento dei dati pubblicati, alla reperibilità dei dati da parte dei motori di ricerca interni ed esterni al sito, al limite temporale della pubblicazione di atti e dati, alle cautele rispetto alla possibilità di duplicazione massiva dei dati da parte degli utenti.

Da ultimo, tra i principali requisiti normativi cui il progetto sarà conforme, si richiamano le specifiche Leggi Regionali:

- Regione Abruzzo: L.R. del 14 marzo 2000, n. 25 Legge generale sulla società dell'informazione
- Regione Basilicata: L.R. del 4 novembre 1996, n. 53 Legge generale sulla società dell'informazione
- Regione Emilia Romagna: L.R. del 24 maggio 2004, n. 11 Legge generale sulla società dell'informazione

- Regione Friuli Venezia Giulia: L.R. del 9 gennaio 2006, n. 1 (Principi e norme del sistema Regione-EELL), L.R. del 18 maggio 2006, n. 8 (Diffusione cultura informatica)
- Regione Lazio: L.R. del 3 agosto 2001, n. 20 Istituzione società regionale per l'informatica
- Regione Liguria: L.R. del 18 Dicembre 2006, n. 42 Legge generale sulla società dell'informazione
- Regione Molise: L.R. del 27 gennaio 1999, n. 3 Informatizzazione uffici e servizi regionali
- Regione Piemonte: L.R. del 26 marzo 2009, n. 9 Legge sul pluralismo informatico, software libero e portabilità dei documenti informatici
- Regione Sicilia: L.R. del 3 maggio 2001, n. 6 (Istituzione del Coordinamento sistemi informativi), L.R. del 27 aprile 1999, n. 10 (Razionalizzazione spesa informatica)
- Regione Toscana: L.R. 26 gennaio 2004, n. 1 (Legge generale sulla società dell'informazione), L.R. 5 ottobre 2009, n. 54 (Istituzione del sistema informativo e del sistema statistico regionale)
- Regione Umbria: L.R. 31 luglio 1998, n. 27 (Legge generale sulla società dell'informazione), L.R. 25 luglio 2006, n. 11 (Legge sul pluralismo informatico, software a sorgente aperto e portabilità dei documenti informatici)
- Regione Valle d'Aosta: L.R. 12 luglio 1996, n. 16 Legge generale sulla società dell'informazione
- Regione Veneto: L.R. del 14 novembre 2008, n. 19 Legge sul pluralismo informatico, riuso, formati aperti e standard

Come risulta evidente, l'elevata vivacità dell'evoluzione delle norme che governano il settore dell'E-Government, dimostrata negli ultimi anni, richiede che il sistema PEOPLE LPCE possieda una spiccata flessibilità nell'adattarsi a esigenze e specifiche sempre nuove.



L'elemento ritenuto più importante (peso 5) è la *Sicurezza applicativa finale*, mentre la *Conformità ai criteri di accessibilità* è quella considerata meno determinante (peso 1).

Per colonna abbiamo invece i **Functional Requirements**, ovvero i requisiti funzionali che si desidera che il prodotto possieda: nel caso specifico si è spaziato dalla *compatibilità* con i più diffusi browser, alla *portabilità* fino agli aspetti di *supporto e documentazione*.

Una volta stabiliti gli elementi di riga e di colonna, si procede con l'analisi di *se, come e quanto intensa* è la **correlazione** tra ciascun requisito funzionale e le singole esigenze dell'utilizzatore. I risultati di questa operazione sono contenuti, sia algebricamente che graficamente, nella parte centrale della matrice, in ogni cella di incrocio tra riga e colonna. Se non vi è correlazione tra gli elementi la cella viene lasciata vuota, altrimenti, a seconda dell'intensità e del verso del legame, viene inserito un valore da -9 (correlazione fortemente negativa) a +9 (fortemente positiva).

E' piuttosto immediato comprendere che un requisito tecnico fortemente correlato alle più importanti esigenze, acquisterà a sua volta un peso maggiore (positivamente se la sua correlazione è positiva, negativamente nel caso opposto). Il peso di ciascun requisito tecnico, infatti, non è assegnato a priori, ma è stabilito obbiettivamente in virtù della sua correlazione con le esigenze dell'utilizzatore e, quindi, con il peso che a queste ultime è stato inizialmente associato.

Il risultato di questa delicata operazione è quindi l'ottenimento di un peso (assoluto e relativo) per tutti i requisiti funzionali, denominato **Technical Importance Rating**. Nel nostro caso specifico, la *Monocodifica dei sorgenti*, essendo fortemente correlata ad esigenze con peso rilevante, ottiene il maggior peso tra tutti i requisiti tecnici.

Una volta determinato il peso relativo (in percentuale) di ciascun requisito, viene effettuata una valutazione tecnica sulla rispondenza di ogni prodotto confrontato ai requisiti tecnici richiesti. Il grado di soddisfazione dei requisiti viene valutato secondo una scala da 0 a 5, col seguente significato:

5, *Facilmente raggiungibile o già raggiunto*

4, *Difficoltà tecnica limitata*

3, *Problemi tecnici limitati, costi ragionevoli*

2, *Problemi tecnici limitati, alti costi*

1, *Difficilmente raggiungibile e altamente costoso*

0, *Praticamente irraggiungibile per difficoltà e costo*

Per giungere alle corrette considerazioni, le valutazioni assolute devono essere messe in relazione con i pesi tecnici precedentemente calcolati, ottenendo un punteggio ponderato al grado di importanza. Si giunge così ai punteggi finali, che mostrano come punteggi assoluti anche molto bassi, siano pressoché irrilevanti in termini relativi se associati ad un peso modesto.

La somma di tutti i punteggi ponderati determina lo **Score medio**, ovvero il punteggio globale sul prodotto, che determina la scelta di Vaadin

E' necessario sottolineare che la matrice QFD è stata applicata in uno scenario non tradizionale: generalmente, infatti, tale modello viene adottato nei settori di produzione per valutare le caratteristiche di un proprio prodotto, attraverso la misura della rispondenza a certe aspettative degli utenti, effettuando confronti con prodotti simili offerti dalla concorrenza.

In questo caso, invece, non essendoci uno sviluppo in proprio, l'intera rosa dei prodotti valutati sono da considerarsi della concorrenza. Per lo stesso motivo, il decisore riveste in questo modello il ruolo sia di produttore che di utilizzatore: quelle che nell'accezione classica sono considerate le esigenze del cliente, corrispondono in questo contesto alle esigenze stesse della soluzione, perché ciò che il decisore cerca nel prodotto sono le caratteristiche che garantiscano la soddisfazione dei requisiti imposti.

Il QFD adottato ha quindi la valenza di un modello con cui "presentare", attraverso un diagramma analitico ben strutturato, le motivazioni e le evidenze determinanti che hanno portato ad una determinata scelta.