Liguria Digitale

Sede Legale:
VIA MELEN 77 - 16152 GENOVA
Tel +39 - 01065451 - Fax +39 - 0106545422

UFFICI DI PROSSIMITÀ (GPROX)

ARCHITETTURA DEL SISTEMA

DATI DI CONTROLLO DEL DOCUMENTO

Oggetto:	Architettura del Sistema
Riferimenti a documenti aziendali:	
Riferimenti esterni:	
Moduli utilizzati:	nessuno
Pagine variate:	nessuna

INDICE

1 INTRODUZIONE 4
1.1 Premessa 4
1.2 Scopo 4
1.3 Area di applicazione 4
2 REQUISITI ARCHITETTURALI DI RIFERIMENTO 5
2.1 I principi di design definiti dalle Linee guida per i servizi digitali della PA 5
2.1.1 La Service Design 5
2.1.2 La Content Design 6
2.1.3 La User Research 6
2.1.4 La User Interface Design 7
3 ARCHITETTURA FUNZIONALE DEL SISTEMA 8
3.1 Aspetti normativi e tecnici di riferimento 8
3.2 Stakeholders e attori del sistema 8
3.3 Scenari d'uso principali 10
4 ARCHITETTURA APPLICATIVA DELLA PIATTAFORMA 13
4.1 La scelta del paradigma architetturale 16
4.2 I contesti di Frontend 18
4.3 I contesti di Backend 18
5 ARCHITETTURA DI DEPLOYMENT DELLA PIATTAFORMA 19
5.1 Schema dell'architettura di esercizio 19

1 INTRODUZIONE

1.1 Premessa

Il presente documento rappresenta la descrizione dell' Architettura del Sistema Uffici di Prossimità (GProx)

1.2 Scopo

Scopo di questo documento è illustrare l'architettura funzionale e tecnica del sistema informatico a supporto del progetto Giustizia di prossimità (nel seguito indicato con GProx).

1.3 Area di applicazione

Il presente documento viene applicato dalle strutture di Software Factory and Innovation e dalla Divisione Sanità di Liguria Digitale S.p.A.

2 REQUISITI ARCHITETTURALI DI RIFERIMENTO

2.1 I principi di design definiti dalle Linee guida per i servizi digitali della PA

In coerenza con le "Linee guida di design per i servizi digitali della PA" (https://docs.italia.it/italia/designers-italia/design-linee-guida-docs/it/stabile/), la progettazione dell'ambiente digitale, che caratterizza lo Uffici di Prossimità (GProx), ha compreso un insieme di attività di analisi architetturale:

- La *Service Design*: ovvero la progettazione dei servizi di dominio. L'ambito è quello dell'architettura funzionale del sistema.
- La *Content Design*: ovvero la progettazione dei contenuti. L'ambito è quello dell'architettura dell'informazione gestita dal sistema.
- La *User Research*: ovvero l'analisi di usabilità. L'ambito è quello dell'architettura della comunicazione fornita dal sistema.
- La *User Interface Design*: ovvero l'analisi delle interfacce utente, personalizzate sulla base delle necessità dei soggetti fruitori, in conformità con gli standard che sono oggi richiesti da AGID. L'ambito è quello dell'architettura dell'interazione con gli utenti del sistema.

2.1.1 La Service Design

La *Service Design* ha considerato i requisiti funzionali coerentemente con lo scenario organizzativo esistente focalizzandosi sulla digitalizzazione dei processi interni e all'erogazione di servizi digitali direttamente all'end user (ovvero al cittadino) che diventa, in questo contesto, parte attiva e consapevole nei processi che lo riguardano. Ciò è in linea con i requisiti caratteristici del Piano Triennale per l'Informatica nella Pubblica Amministrazione dell'Agenzia per l'Italia digitale (AGID).

Ha tenuto conto inoltre del panorama tecnologico che oggi è a disposizione delle infrastrutture ICT, degli operatori e dei cittadini.

In quest'ottica sono emersi quindi i requisiti funzionali e non funzionali del sistema, e che sono stati associati alle nuove opportunità di erogazione del servizio

Esempi di opportunità sono:

- Le infrastrutture immateriali, come le Piattaforme Abilitanti di autenticazione SPID/CIE e Pago PA, l'Anagrafe Nazionale della Popolazione Residente ecc.
- La Piattaforma di API management Regionale
- Il diffondersi capillare dell'utilizzo di device mobili fra i cittadini
- L'estendersi della copertura delle reti a banda larga

L'esecuzione di una corretta *Service Design* è stato l'elemento fondamentale per la fase di progettazione dell'architettura tecnica basata sulla separazione dei diversi componenti applicativi e più in particolare sulla separazione fra i livelli di frontend e di backend che dialogano attraverso opportune API specifiche del dominio integrandone alcune "di backbone", che sono trasversali al Sistema Informativo Regionale.

2.1.2 La Content Design

La *Content Design* si è occupata dell'organizzazione semantica e logica dei concetti informativi che vengono gestiti e trasferiti dal sistema agli utenti. Anche la *Content Design*, come la Service Design, ha tratto origine dai concetti informativi già attualmente gestiti dai processi esistenti, e si è focalizzata sul disegnare l'architettura dell'informazione in ottica "user centered".

Come riportato nelle Linee Guida AGID, la *Content Design* è consistita nello svolgimento delle attività di progettazione della navigazione delle interfacce, sia di backoffice che di frontoffice, della progettazione dei contenuti informativi e della progettazione dei flussi di interazione con l'utente.

Le attività di progettazione dell'architettura dell'informazione è partita dalla definizione dei profili degli utenti del Sistema e dell'individuazione dei relativi bisogni all'interno del dominio, ovvero dalle necessità operative di fruizione e di gestione delle informazioni, proseguendo con la definizione dei contenuti strutturati e non strutturati che il Sistema dovrà gestire e veicolare attraverso le diverse interfacce (utente, API ecc.).

Particolare attenzione è stata posta nella definizione dei criteri di sicurezza all'accesso ai diversi contenuti da parte dei differenti soggetti fruitori, in particolare alla gestione dei dati personali con misure adeguate al rispetto della privacy (privacy-by-design) evitando i rischi di esposizione di contenuti informativi a soggetti non autorizzati ed evitando l'eccedenza del contenuto trasmesso rispetto a quanto previsto dallo specifico trattamento.

Come già descritto nel precedente sotto paragrafo dedicato alla descrizione della Service Design, nell'ottica dell'obiettivo di realizzare servizi diretti ai cittadini, la progettazione del Sistema non ha compreso solo la progettazione delle funzionalità amministrative di frontoffice e di backoffice rivolte agli operatori istituzionali ma ha integrato la progettazione delle funzionalità di accesso alle informazioni all'utente finale del servizio.

In quest'ottica la *Content Design* si è adattata correttamente al contesto di riferimento e alla tipologia di utente a cui il Sistema si rivolgerà e si è basata sull'utilizzo di standard nella definizione dei contenuti, dei dati e della loro classificazione, che è alla base dell'interoperabilità e che in definitiva (cfr. Linee Guida) *"[…] rappresenta la creazione di un linguaggio digitale comune alla Pubblica Amministrazione italiana".*

2.1.3 La User Research

La *User Research*, come definito nelle Linee Guida AGID, è l'elemento fondamentale per la progettazione di quelle componenti del Sistema che si rivolgono prevalentemente all'utente cittadino, ovvero, come verrà illustrato più avanti, alla componente di Portale del Sistema.

Partendo dal servizio offerto, la User Research quindi si è andata ad occupare primariamente dell'usabilità, vista come (cfr. Linee Guida) *"[…] un costrutto misurabile"* del grado di efficacia, ovvero del grado in cui l'utente riuscirà a completare le operazioni richieste per raggiungere il proprio obiettivo in modo corretto e completo, di efficienza ovvero della quantità di risorse che la persona spenderà nelle operazioni richieste per raggiungere un dato obiettivo e della soddisfazione soggettiva, che è la dimensione più complessa da valutare e da raggiungere, poiché riguarda il livello di gratificazione che l'esperienza d'uso offre. (cfr. Linee Guida) *"[…] Un sistema può funzionare molto bene ma può non bastare a rendere l'interazione confortevole e piacevole. Rientrano in questa dimensione aspetti come l'estetica, la qualità relazionale".*

2.1.4 La User Interface Design

La *User Interface Design* è l'analisi dell'insieme di quegli elementi con i quali l'utente (operatore, cittadino) interagirà per ottenere i servizi digitali offerti dal sistema.

Il sistema, nei suoi diversi componenti di frontend presenta una interfaccia grafica (GUI) moderna e responsive, fruibile sia da apparati desktop che da device mobili, con l'obiettivo di fornire un'esperienza di utilizzo ottimale indipendentemente dal tipo di dispositivo utilizzato e consentendo in ogni situazione facilità di lettura e navigazione.

L'approccio è tale da garantire la responsività dell'applicazione e l'impiego ottimale delle indicazioni fornite, ciò avverrà attraverso l'utilizzo dei temi forniti dai "Web Kit" di Designers-Italia come decritto nel capitolo dedicato delle Linee Guida (https://docs.italia.it/italia/designers-italia/design-linee-guida-docs/it/stabile/doc/user-interface/lo-sviluppo-di-un-interfaccia-e-i-web-kit.html#i-web-kit-per-lo-sviluppo-dellinterfaccia).

Inoltre il Uffici di Prossimità (GProx) risponde ai requisiti di interfaccia stabiliti da Regione Toscana, riferimento per gli standard grafici nell'ambito del progetto.

3 ARCHITETTURA FUNZIONALE DEL SISTEMA

3.1 Aspetti normativi e tecnici di riferimento

Gli scenari di riferimento per la definizione dell'architettura funzionale dello Uffici di Prossimità (GProx) derivano dalle specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministero della giustizia in data 21 febbraio 2011 n. 44, recante il regolamento concernente le regole tecniche per l'adozione, nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti da decreto legislativo 7 marzo 2005, n.82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2 del decreto-legge 29 dicembre 2009, n.193, convertito nella legge 22 febbraio 2010, n.24

I principali riferimenti normativi sono pertanto:

- Il decreto del 21 febbraio 2011, n. 44, recuperabile all'indirizzo https://www.normattiva.it/uri-res/N2Ls?urn:nir:ministero.giustizia:decreto:2011-02-21;44!vig=
- L'Allegato 1: MODELLO DI DOMANDA DI ISCRIZIONE ALL'ELENCO PUBBLICO DEI PUNTI DI ACCESSO
- La documentazione servizi web esposti per invocazione PdA:recuperabile all'indirizzo: http://pst.giustizia.it/PST/it/pst_26_1.wp?previousPage=pst_26&contentId=DOC568

3.2 Stakeholders e attori del sistema

L'organizzazione del lavoro degli uffici di prossimità coinvolge i seguenti attori principali:

- Il Ministero della Giustizia
    - Colloquia con soggetti abilitati esterni purché il Registro Generale degli Indirizzi Elettronici (ReGIndE), gestito dal Ministero stesso, contenga i dati identificativi nonché l'indirizzo di posta elettronica certificata (PEC) di tali soggetti, e che sono:
        - Gli appartenenti ad un ente pubblico
        - I professionisti iscritti in albi ed elenchi istituiti con legge
        - Gli ausiliari del giudice
    - Tiene un elenco pubblico dei punti di accesso. Un punto di accesso costituisce una sorta di ponte, attraverso il quale i soggetti abilitati esterni possono accedere ai servizi offerti dal Sistema Giustizia (in particolare web service del GST Gestore Servizi Telematici esposti tramite proxy dal PST Portale dei Servizi Telematici). I servizi attivi sono elencati nel catalogo dei

servizi telematici. I punti di accesso realizzano autonomamente la parte di front-end relativa ai servizi da richiamare, che deve essere localizzata all'interno della intranet del punto di accesso stesso e non accessibile direttamente dall'esterno. I punti di accesso possono a loro volta esporre i web service forniti dal gestore dei servizi telematici, a beneficio di applicazioni esterne. Tramite un punto di accesso un utente abilitato esterno può accedere alle informazioni del SICID (Sistema Informativo Civile Distrettuale), ottenere copia di documentazione o consultare fascicoli.

- I soggetti abilitati esterni
    - Possono effettuare una trasmissione informatica di atti e allegati ad un ufficio giudiziario: gli atti e gli allegati debbono essere contenuti nella "busta telematica", un file MIME rispondente a specifiche fissate dal Ministero della Giustizia e contenente l'atto firmato e criptato.
- Il personale di ASL, dei Comuni e delle Aziende Ospedaliere (li chiameremo tutti 'funzionari in proprio')
    - Può/deve presentare ricorso per Amministrazione di Sostegno in prima persona ovvero come richiedente per un beneficiario, che sia assistito dai loro servizi sociali o sanitari.
- Il personale che agisce presso gli uffici di prossimità (li chiameremo 'operatori ufficio di prossimità).
    - Appartengono ad un ente pubblico ed hanno il compito di facilitare la presentazione di ricorsi presso i Tribunali da parte di cittadini richiedenti. Quindi, diversamente dai 'funzionari in proprio', gli 'operatori ufficio di prossimità' garantiscono sia al richiedente che al Ministero il trasferimento della corretta documentazione al Tribunale di competenza, ma i richiedenti restano i cittadini che si recano all'ufficio di prossimità. Possiamo dire che garantiscono una "trasmissione telematica affidabile e autorizzata".
- I cittadini.
    - Si recano all'ufficio di prossimità per presentare ricorso presso i Tribunali ed in questo sono supportati dal personale che agisce presso gli uffici di prossimità

3.3 Scenari d'uso principali

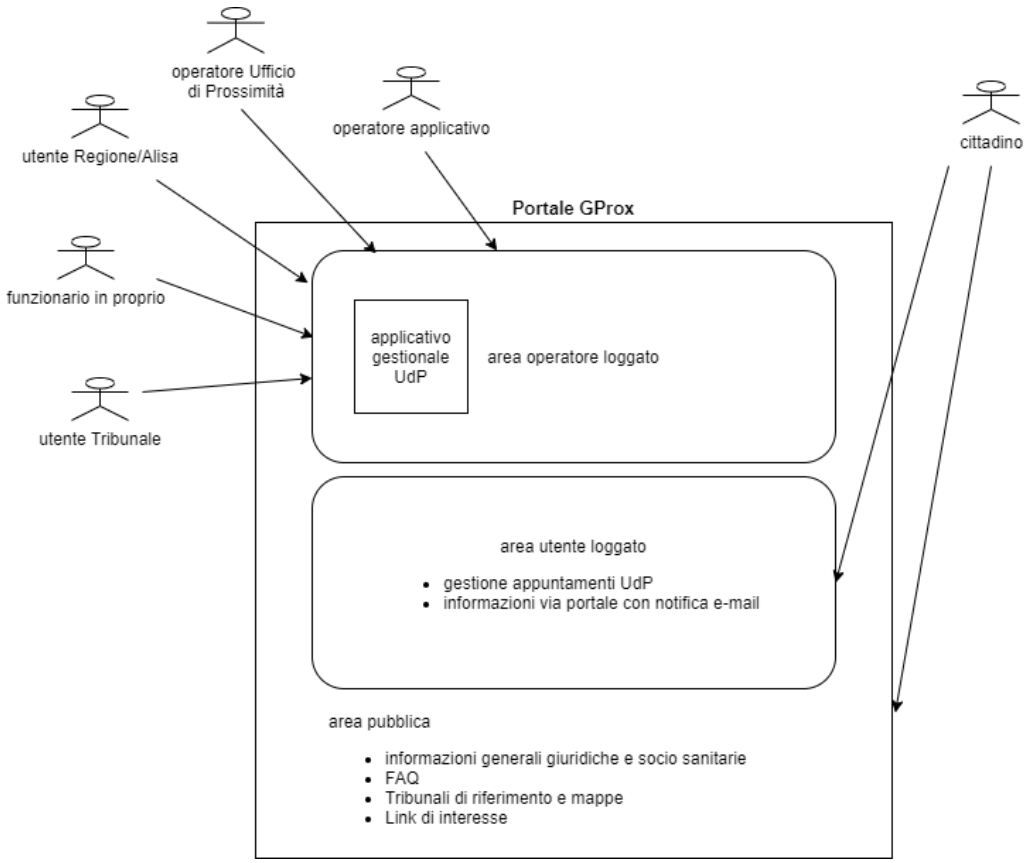
Gli scenari che consentono agli uffici di prossimità di operare e ai 'funzionari in proprio' di veicolare i ricorsi che sono tenuti a presentare, hanno le seguenti caratteristiche.

1. Ogni 'operatore ufficio di prossimità' per svolgere la funzione di tramite tra i cittadini richiedenti e il Ministero nella "trasmissione telematica affidabile e autorizzata":
    a. È registrato su ReGIndE (Registro Generale degli Indirizzi Elettronici) di Giustizia
    b. Ottiene dai singoli richiedenti apposita delega per visibilità e comunicazioni
2. Gli uffici di prossimità sono dal punto di vista organizzativo "uffici dipendenti dal Comune"
    a. Presso cui opera personale dipendente da Comuni e/o Aziende Sanitarie
    b. Con macchine attestate su rete pubblica (non dietro firewall di Comuni o Aziende Sanitarie, indipendentemente da dove siano fisicamente collocate le sedi dell'ufficio)
    c. In cui ogni operatore accede alle funzionalità utili per l'attività dal portale della Giustizia di prossimità accedendo tramite SPID, CNS o CIE.
3. Il personale degli uffici di prossimità per svolgere il lavoro deve pertanto disporre
    a. Di un identità digitale (SPID, CNS o CIE)
    b. Di un accesso alla casella PEC di ufficio (comune a tutti gli operatori dell'ufficio) sul dominio specifico degli uffici di prossimità, rilasciato da Regione
    c. Di una firma elettronica per certificare digitalmente le proprie funzioni rilasciata dall'ente cui appartiene o dalla Regione.
4. Il personale degli uffici di prossimità, in quanto autorizzato, può
    a. Rilasciare copie conformi dei documenti di Giustizia, cui accede essendo abilitato dal Ministero (ReGIndE) e delegato dal cittadino richiedente
    b. 'attestare' i pagamenti.

L'erogazione dei differenti servizi che implementano gli scenari d'uso dello Uffici di Prossimità (GProx) avviene tramite un Portale (Portale Giustizia di Prossimità) che comprende tre aree funzionali differenti:

1. Un'area riservata ad "autenticazione forte" alla quale si accede con credenziali SPID, CNS o CIE, suddivisa in
    a. Una sezione per gli operatori che possono fruire di funzioni applicative sulla base delle abilitazioni dell'utente collegato: operative, di configurazione o di monitoraggio
    b. Una sezione per i cittadini, che fornisce servizi quali:
        i. la gestione degli appuntamenti presso un ufficio di prossimità
        ii. la richiesta di informazioni via e-mail ad un ufficio di prossimità.
2. Un'area pubblica, dove sono reperibili contenuti informativi, mappe interattive per trovare il Tribunale di riferimento e link ai siti dei singoli Tribunali, nonché la modulistica per i ricorsi o gli altri depositi possibili ove sia possibile una standardizzazione a livello regionale, risolvendo il problema della coerenza degli aggiornamenti tra portale di giustizia di prossimità e siti dei singoli Tribunali (altrimenti il portale veicolerà gli utenti sui singoli siti dei Tribunali ove reperire l'informazione. Inoltre sono reperibili contenuti informativi inerenti l'area sociosanitaria, spesso correlata ai temi della volontaria giurisdizione.

Uno schema ad alto livello dell'architettura funzionale del portale è mostrato nella figura seguente:


operatore Ufficio di Prossimità
operatore applicativo
utente Regione/Alisa
cittadino
Portale GProx
funzionario in proprio
applicativo gestionale UdP
area operatore loggato
utente Tribunale
area utente loggato
gestione appuntamenti UdP
informazioni via portale con notifica e-mail
area pubblica
informazioni generali giuridiche e socio sanitarie
FAQ
Tribunali di riferimento e mappe
Link di interesse

4 ARCHITETTURA APPLICATIVA DELLA PIATTAFORMA

La piattaforma è composta da un portale CMS (Content Management System) che rappresenta il punto di accesso a tutte le funzionalità, siano esse pubbliche o ad accesso riservato e da un'applicazione web based "a 3 strati" (applicativo "Giustizia di prossimità"), dedicata all'erogazione delle funzionalità dedicate agli operatori istituzionali con un accesso tramite credenziali forti.

L'utente interagisce con la piattaforma tramite un browser (1° strato).

La componente di business (che rappresenta il 2° strato) è costituita da una web application Java che viene eseguita in un web/application server. Lo strato di persistenza (che rappresenta il 3° strato) ha una struttura tipicamente relazionale ed è contenuto in un RDBMS.

I processi di autenticazione e di autorizzazione all'accesso dell'utente sono delegati ad una Piattaforma di Identity&Access Management (I&AM) regionale (ogni Regione utilizzerà la propria infrastruttura), che provvede a:

- Mediare i processi di autenticazione con gli IdP SPID, CIE e TS/CNS attraverso la federazione SAML con l'infrastruttura nazionale
- Autorizzare l'accesso alle funzioni e ai dati tramite una componente di Access Gateway (AG) attraverso il paradigma RBAC (Role Based Authorization Control), ovvero tramite la verifica di ruoli specifici attribuiti dall'IdP agli utenti che sono previamente censiti nell'eDirectory;
- Applicare ulteriori ACLs per l'accesso da domini riconosciuti, attraverso opportuna configurazione dell'AG;
- Terminare il protocollo sicuro sull'AG (terminazione di HTTPS).

L'utente accede autenticandosi sul Portale posto in Single Sign On (SSO) con l'applicazione web.

L'accesso del browser alle risorse applicative (pagine HTML) dell'applicazione è basato su un meccanismo "reverse proxy", implementato tramite la componente di AG di NAM.

L'AG chiede all'utente di autenticarsi, dirigendo il browser sull' una interfaccia dedicata alla login che media il colloquio con i diversi IdP. Effettuata l'autenticazione vengono validate opportune ACL (ad esempio sul ruolo dell'utente) e viene creata la sessione utente specifica.

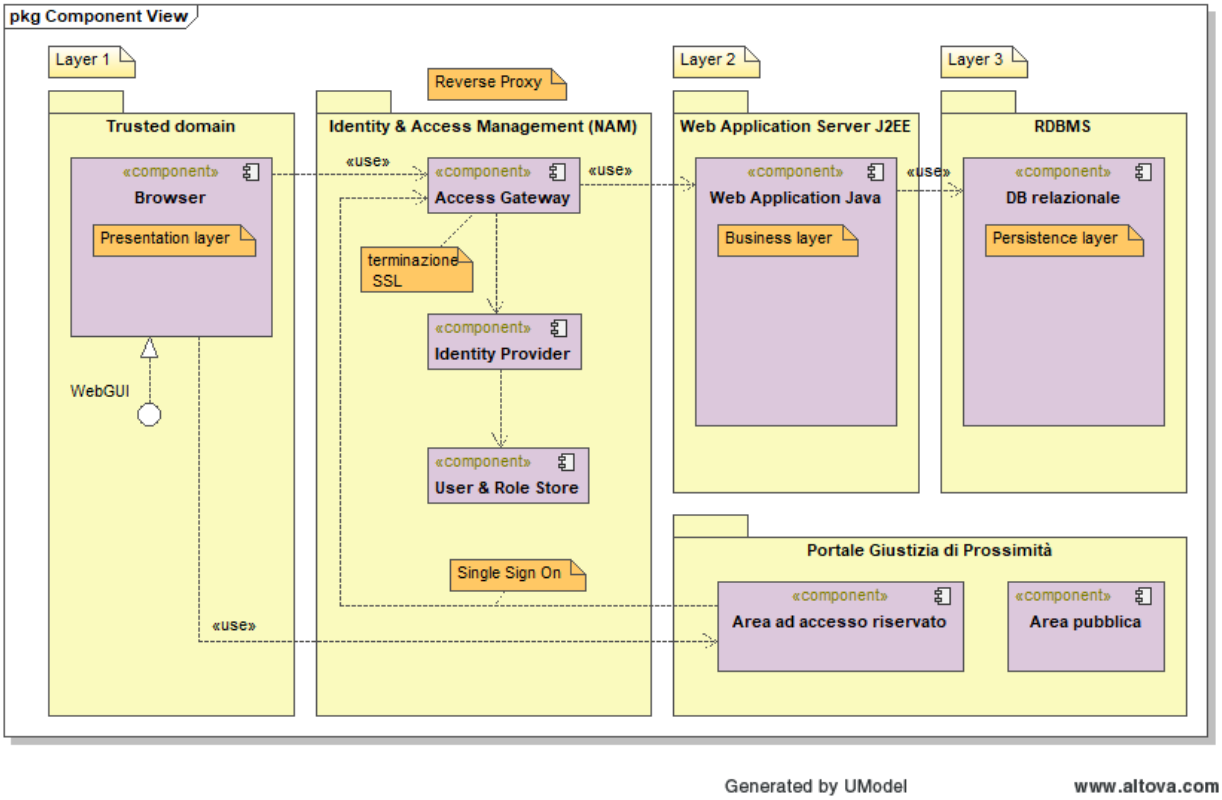
L'AG gestisce per tutta la durata della sessione il traffico request/response fra il browser e l'application server, mascherando al primo l'indirizzo IP del secondo (reverse proxy), terminando il protocollo HTTPS verso il browser e iniettando un set di opportuni header nelle request http verso l'application server che contengono informazioni sull'utente prelevate dallo store in fase di autenticazione.

La sessione è specifica dell'istanza del browser dell'utente, ovvero diversi utenti concorrenti non condividono la medesima sessione. Alla logout l'AG cancella la sessione utente ed in tal modo un successivo accesso da quel browser potrà avvenire solo attraverso il ripetersi della fase di autenticazione e autorizzazione.

Per ogni tipologia di utente è inoltre applicato un determinato profilo a livello applicativo, che fornirà accesso a determinate e specifiche funzionalità.

Tutte le logiche di processo sono eseguite all'interno di un application server, ovvero all'interno di una Java Virtual Machine, che si occupa inoltre di gestire il pool di connessioni al database relazionale RDBMS.

Nella figura seguente è mostrato uno schema di sintesi dell'architettura applicativa del Sistema attuale.



Il portale ha un'area per la consultazione pubblica ed una ad accesso SPID: per il cittadino che consente di fissare appuntamenti presso gli uffici di prossimità, oppure di formulare quesiti; per l'operatore di sportello che abilita in base alla profilazione alle altre componenti del sistema.

Realizzato tramite il CMS Joomla e per la registrazione degli utenti si appoggia ad una base dati mysql. Per rendere disponibili le funzionalità si interfaccia tramite API ad alcuni servizi Restful esposti dal backend della componente di backoffice

Nella componente web application sono contenuti

1. Configuratore: è l'applicativo con cui si configura il sistema. Tramite il configuratore è possibile popolare le anagrafiche delle strutture degli operatori, dei profili e le abilitazioni degli operatori sui progetti mediante i profili. Sviluppata in java 8, si appoggia al framework Apache wicket 7 e ad una base dati postgreSQL versione 12.
2. GProx: è l'applicativo con cui l'operatore può gestire il calendario dell'ufficio di prossimità, le disponibilità. Inoltre prende in carico il caso e raccoglie la documentazione richiesta per il deposito al tribunale di competenza territoriale. le sue caratteristiche principali sono:
    a. Sviluppato in java 8, la componente di frontend si appoggia al framework Apache wicket 8.
    b. La parte di backend si appoggia ad una base dati postgreSQL versione 12.
    c. Frontend e backend comunicano tramite API RESTful con payload json
3. Redattore Atti: è la componente che si interfaccia con Gprox per il recepimento delle informazioni necessarie al deposito in tribunale. L'applicazione raccoglie la documentazione dell'atto, alcuni documenti vanno firmati digitalmente, compone la busta cifrata con la chiave pubblica del tribunale destinatario e infine effettua il deposito in tribunale, mediante PEC. Comunica con GProx tramite API RESTful con payload json.

I requisiti di pila tecnologica sono:

- CMS Joomla: ultima versione disponibile
- PHP: versione 8.0 (minimale 7.2.5)
- db mysql: versione 5.6 + (minimale 5.6)
- Java: versione 1.8
- JBoss Wildfly 12
- PostgreSQL 12

4.1 La scelta del paradigma architetturale

L'architettura tecnica di riferimento è basata sul paradigma *"API first"*, che garantisce la necessaria separazione dei livelli di back end e front end attraverso l'impiego di logiche aperte e di standard, in modo da garantire anche ad altri attori diversi da quelli attuali, pubblici e privati, accessibilità e massima interoperabilità dei dati e dei servizi resi disponibili.

Lo stile architetturale a servizi è sostanzialmente un approccio allo sviluppo di una singola applicazione vista come insieme di piccoli servizi, ciascuno dei quali viene eseguito da un proprio processo e comunica con altri servizi via HTTP API. Ogni servizio è un'entità separata e la comunicazione avviene attraverso la rete, al fine di garantire l'indipendenza tra i servizi ed evitare ogni forma di accoppiamento (principio di "loose coupling").

Visto dall'esterno ogni servizio si propone quindi come una black-box, esponendo solo un'interfaccia (API), astraendo rispetto al dettaglio di come le funzionalità sono state implementate e dallo specifico linguaggio utilizzato. Un vantaggio immediato di questo approccio è che il cambiamento di ciascun servizio non avrà impatto sugli altri.

Questo approccio nella definizione della nuova architettura applicativa permette di:

- *Velocizzare i tempi di rilascio del software e reagire più velocemente a nuove esigenze.* Siccome ogni singolo servizio è autonomo rispetto agli altri, può raggiungere l'ambiente di produzione in modo indipendente dagli altri, senza che tale attività abbia effetti drammatici sul resto del sistema. Attraverso un processo di deployment snello e veloce questo approccio consente di poter aggiungere o modificare funzionalità al software in modo più efficace ed efficiente.
- *Ottenere maggiore resilienza.* In un'architettura a servizi, quando una componente non funziona non è automatico che tutto il sistema software smetta di funzionare. Nella maggior parte dei casi è possibile isolare il problema ed intervenire mentre il resto del sistema continua a funzionare, cosa non possibile nell'attuale architettura monolitica.
- *Scalare a livello di singola funzione* In generale risulta molto più semplice ed economico scalare un servizio rispetto ad un sistema software monolitico di maggiori dimensioni. Il modello a servizi consente di poter effettuare provisioning delle parti del sistema software in modo dinamico ed intelligente.
- *Agevolare le attività di deployment*. Modificare poche righe di codice su un sistema software monolitico come quello attuale ed effettuarne il deploy è generalmente un'attività non banale, che espone a rischi significativi considerando anche l'impatto che tali modifiche possono avere. Questa paura generalmente porta a raccogliere un certo numero di modifiche prima di avviare un'attività così onerosa e rischiosa. Con l'approccio a servizi ogni singolo servizio può raggiungere l'ambiente di produzione in modo indipendente, sicché se si verifica un problema

esso è facilmente isolato e possono essere intraprese azioni di rollback più velocemente.

- *Comporre elementi*. Tra le opportunità più interessanti dell'architettura a servizi vi è la possibilità di riusare le funzionalità. Infatti è possibile che uno stesso servizio venga utilizzato in modi differenti e per scopi diversi.
- *Facilitare le operazioni di sostituzione*. Quando un sistema software è organizzato a servizi, il costo di sostituire un servizio con un altro più efficiente e migliore è limitato poche giornate di sviluppo, così come banale è il costo di rimuovere un servizio inutile.

Il modello così realizzato ha la caratteristica di separare le logiche di esecuzione dei servizi (strato di backend) dalla loro fruizione (strato di frontend) da parte dei diversi attori.

Lo *strato di backend*, in particolare, mostra le seguenti caratteristiche principali:

1. I singoli componenti software che realizzano i diversi servizi vengono eseguiti in modo autonomo e si basano ciascuno sul principio di singola responsabilità (SRP).
2. Ogni componente espone le proprie funzionalità ad altri componenti in modalità REST API
3. Ogni componente agisce sul proprio domino delle entità di persistenza ed è responsabile della corretta gestione delle stesse in termini di sicurezza dei dati trattati
4. Comprende uno strato applicativo di orchestrazione e di automazione dei diversi scenari del processo amministrativo sottostante, deputato al cosiddetto *"traffico orizzontale"*, ovvero alla gestione del dialogo fra i diversi componenti software attraverso le interfacce REST API da ciascuno pubblicate.
5. Sfrutta l'Infrastruttura di Interoperabilità Regionale per:
    a. Fruire delle API di backbone
    b. Pubblicare le proprie API per i frontend del Sistema ovvero per il cosiddetto *"traffico verticale".*
6. Tutti i componenti vengono sviluppati in codice aperto immediatamente eseguibile e pertanto facilmente pubblicabili in modalità di riuso sul portale di Developers Italia.

Lo *strato di front end* invece ha le seguenti caratteristiche:

1. Comprende più applicazioni client dedicate all'accesso da parte dei differenti attori del sistema
2. Le applicazioni implementano i temi di design definiti a livello nazionale (https://developers.italia.it/it/designers/)

3. Dialogano con lo strato di backend attraverso le interfacce API REST che sono da esso esposte
4. Permettono l'accesso autenticato tramite credenziali SPID e/o CIE integrando le funzionalità offerte dalla Piattaforma di autenticazione

4.2 I contesti di Frontend

I contesti di frontend hanno al loro interno tutti i componenti deputati all'interazione con le diverse tipologie di utente.

Tutti i client di frontend richiedono all'utente di eseguire una procedura di autenticazione o con credenziali SPID (o CIE), che viene effettuata attraverso l'Infrastruttura Regionale NAM (*BC Access Management*), o attraverso credenziali rilasciate attraverso il processo di autoregistrazione.

Il componente di *Login* del relativo contesto integra i differenti provider SPID (e CIE) attraverso lo scambio di un'asserzione di identità SAML. L'asserzione di identità però non comprende informazioni di tipo autorizzativo, ma solo di identità (ovvero il codice fiscale dell'utente).

E' stato pertanto necessario comprendere nell'architettura una componente di gestione e di verifica delle autorizzazioni ovvero la verifica dei ruoli associati all'utente, per permettergli l'accesso alle relative funzionalità (componente BIC).

4.3 I contesti di Backend

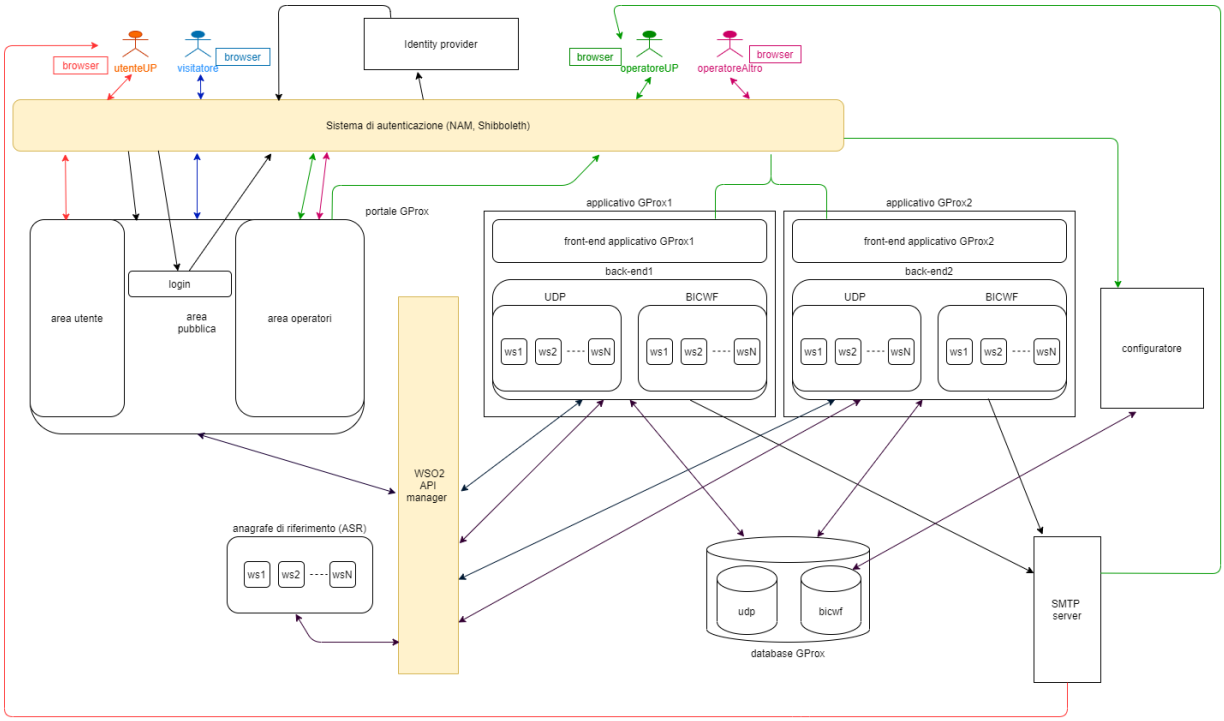
I contesti di backend hanno al loro interno tutti i componenti software deputati all'esecuzione delle logiche di processo applicative nel singolo dominio di responsabilità, e alla gestione delle relative entità di persistenza.

Interagiscono con i componenti di frontend tramite specifiche API Rest, fra qui quelle dispiegate nel dominio di API Management Regionale (basato su piattaforma WSO2) per implementare il cosiddetto traffico verticale.

5 ARCHITETTURA DI DEPLOYMENT DELLA PIATTAFORMA

5.1 Schema dell'architettura di esercizio

Nella figura seguente è mostrato uno schema dell'architettura di esercizio dispiegata per erogare i servizi della piattaforma.



I differenti profili utente dialogano tramite il browser sia con il portale che con la componente applicativa attraverso un processo di autenticazione in Single Sign On (SSO) gestito dal sistema di autenticazione.

Il sistema di autenticazione è in HA e ridondato nelle sue componenti di Access Gateway, che agisce come reverse proxy rispetto alla richiesta delle risorse, e di identity server, che implementa il protocollo di interscambio SAMLP con i differenti Identity Providers.

Il portale è dispiegato in un'architettura LAMP (Linux Apache PHP, MySQL) a sua volta è composto dalle tre aree: utente cittadino, operatore, area pubblica. Invoca un set di API Rest pubblicate dalla Piattaforma di API Management regionale realizzata tramite infrastruttura WSO2 API Manager (versione 2.6).

La componente applicativa comprende sia le applicazioni di frontend che quelle di backend e sono dispiegate su due Application Server Wildfly, su sistema operativo linux, bilanciati

in configurazione attivo-passivo (configurazione di fault tolerance) attraverso un bilanciatore (Fortigate).

La componente di persistenza è dispiegata su RDBMS postgres e comprende i diversi database funzionali ai servizi erogati e ai processi autorizzativi e di profilazione dell'operatore.

Completa l'architettura di deployment un SMTP server (dominio regione.liguria.it) per l'invio di notifiche e interscambio di email.