

# Allegato n. 4

## Sistema di gestione documentale dell'Amministrazione

### Dati identificativi del Sistema di gestione documentale

Si riportano di seguito i dati identificativi del Sistema di gestione documentale:

- Denominazione: SINFONIA – Protocollo
- Fornitore: Maggioli Spa
- Versione: 1.0

### Architettura tecnologica

Il sistema “SINFONIA – Protocollo” è basato su piattaforma SIMEL2, una soluzione software inclusa nel catalogo del software open source a disposizione della Pubblica Amministrazione pubblicato sul portale [developers.italia.it](https://developers.italia.it) e che rispetta le misure minime di sicurezza ICT emanate da AgID, come confermato dalla scheda di dettaglio raggiungibile al seguente link: [SIMEL2](#).

### Architettura Logica della soluzione applicativa

La piattaforma SIMEL 2 si compone di più moduli applicativi. In particolare, “SINFONIA – Protocollo” sfrutta i moduli di Gestione Documentale e Protocollo messi a disposizione da SIMEL2. Il modello architetturale è modulare e prevede vari livelli di astrazione che permettono un aggiornamento tecnologico costante per garantire alti standard di sicurezza sorpassando il problema dell'obsolescenza tecnologica.

### Architettura ad alto livello

L'architettura è stata pensata prima di tutto considerando gli aspetti legati alla sicurezza.

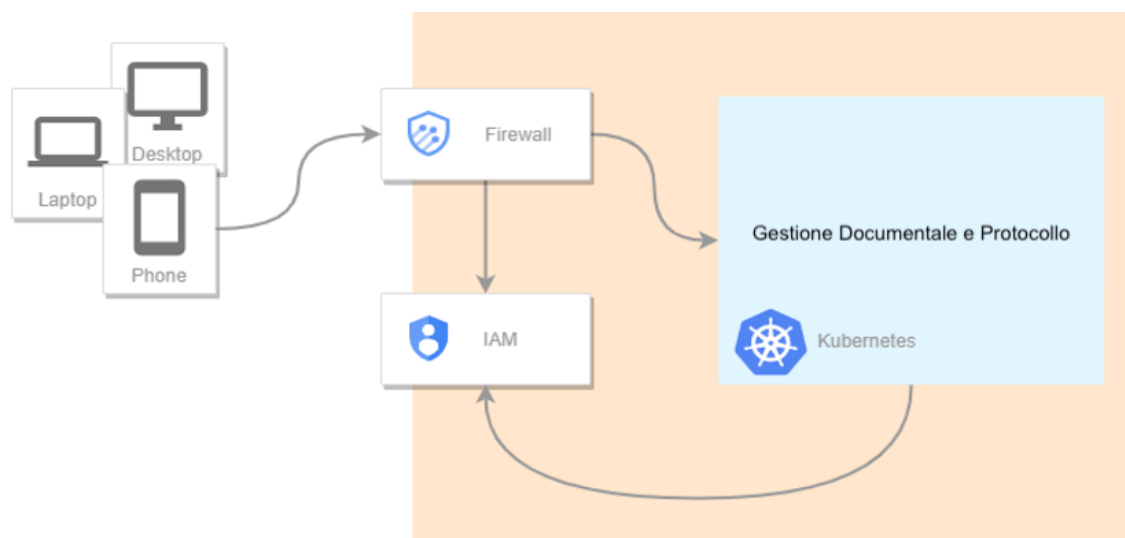


Figura 1: Architettura ad alto livello complessiva

Il perimetro di “SINFONIA – Protocollo” è protetto da un Firewall e tutte le interazioni utente e applicative del sistema sono protette da token autorizzativi rilasciati dal sistema di Identity and Access Management (IAM). Questo elemento gestisce le identità e le credenziali di accesso rilasciando i token JWT che vengono poi utilizzati per autorizzare ogni singola chiamata. Il protocollo standard di autorizzazione con lo IAM è di tipo OAuth2 ma vengono supportate anche altre modalità di comunicazione come SAML. IAM offre varie modalità di integrazione, tra cui autenticazione con credenziali, LDAP, SPID e CIE. Inoltre, è possibile estendere questi metodi integrando moduli di identity management di terze parti come, ad esempio, sistemi regionali o proprietari forniti da altri software.

Per garantire livelli ottimali di operatività e di resilienza a picchi di carico e aggiornamenti software, l'applicativo viene distribuito sfruttando la tecnologia della containerizzazione e l'orchestrazione di container.

### Gestione documentale e protocollo

Il cluster dedicato alla gestione documentale e protocollo espone tutte le funzionalità per la gestione del protocollo, della scrivania utente e dei flussi documentali. L'applicazione ha una robusta e consolidata architettura multi-tier in cui sono previsti gli strati di presentation, business logic e data persistence.

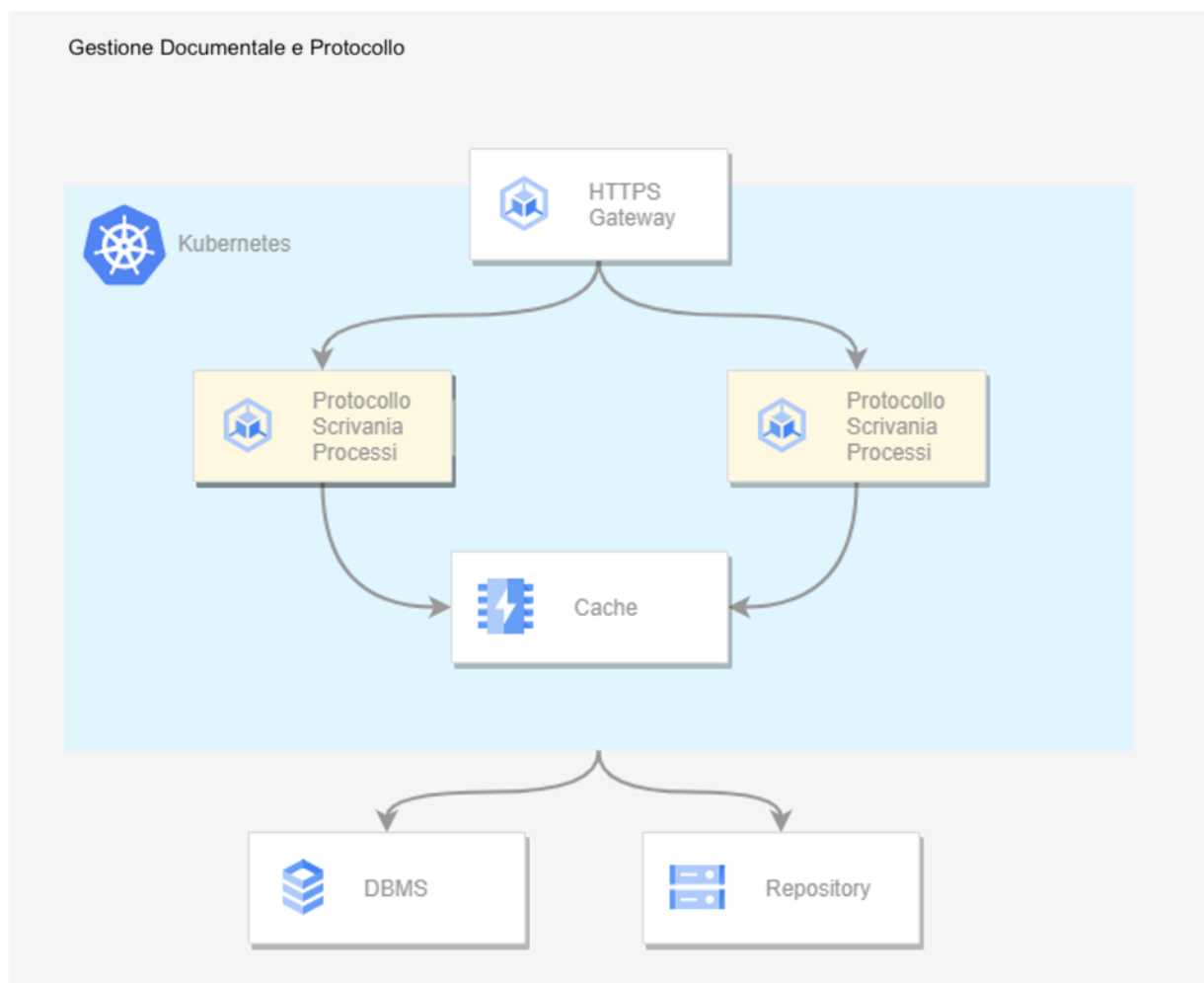


Figura 2: Architettura Gestione Documentale e Protocollo

I livelli di presentation e business sono distribuiti all'interno di un unico container mentre i servizi di persistenza quindi DBMS e Storage sono dispiegati all'esterno del cluster. Il traffico in ingresso viene

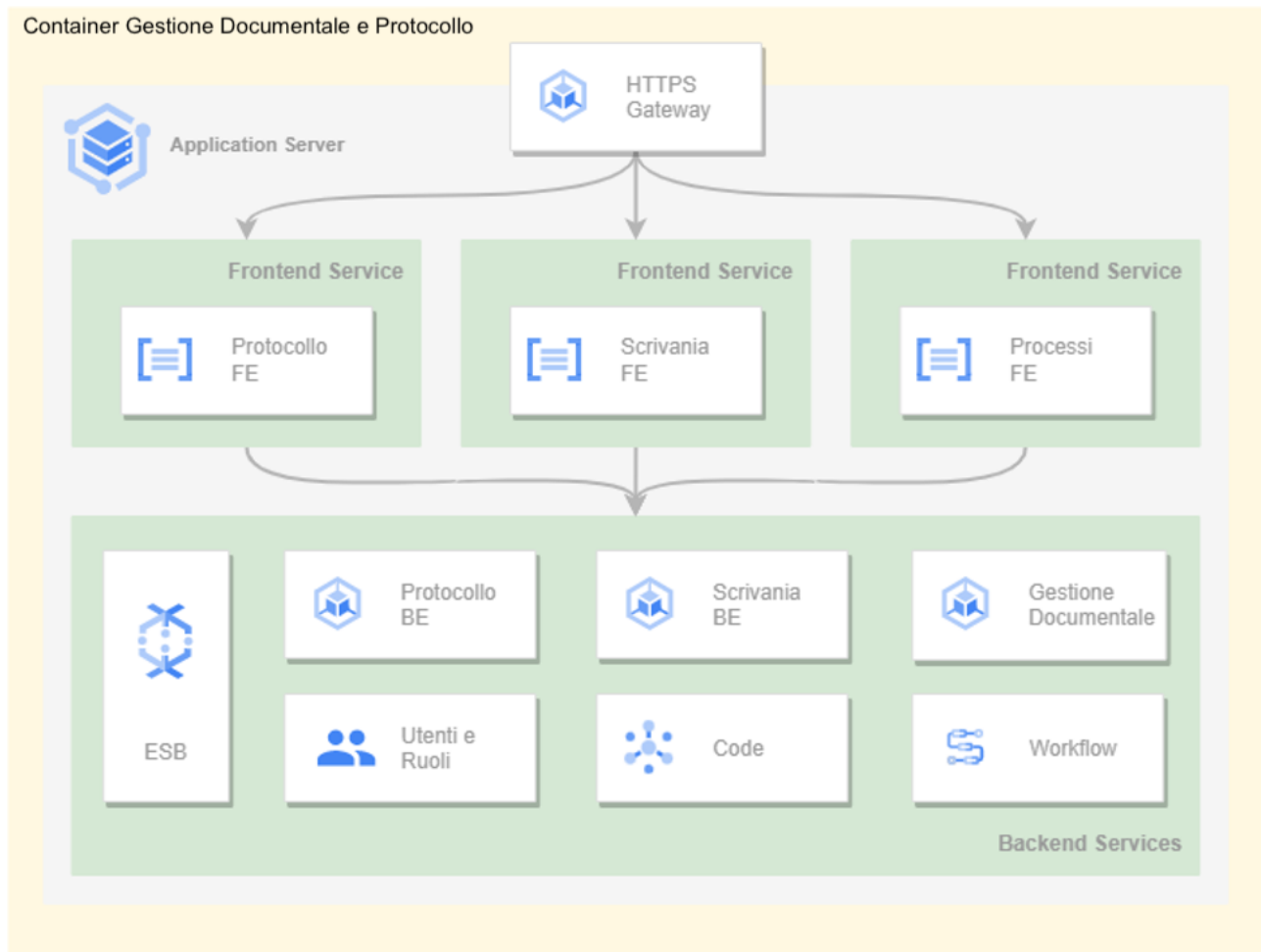


Figura 3: Applicazione del container di Gestione Documentale e Protocollo

veicolato da un gateway HTTPS mentre le varie istanze del container condividono dati e sessioni di lavoro tramite una cache condivisa e presente all'interno del cluster. per ottimizzare le performance.

Il container applicativo contiene i tier di presentation e di business identificati nel diagramma rispettivamente come servizi di frontend e di backend. I servizi di backend beneficiano di tutta la solidità dell'infrastruttura di sicraweb in grado di offrire la gestione degli utenti, organigramma e relativa profilatura dei permessi, la gestione documentale, la gestione delle code di notifica, il workflow per l'elaborazione degli iter di processo e di un service bus per il dispatching dei messaggi scambiati tra i vari moduli applicativi. I servizi di business sono quelli tipici di gestione del protocollo, della scrivania operatore e di gestione e definizione degli iter.

Il presentation tier è implementato tramite un'applicazione web di tipo single page application e a livello architetturale è distribuito tramite applicazioni specifiche per i moduli funzionali. Ogni applicazione espone il bundle con gli elementi di UI necessari per eseguire le specifiche funzioni all'interno della single page application e i servizi di recupero dati che disaccoppiano la logica di business da quella di presentation ottimizzando il traffico dati tra il dispositivo dell'operatore e il cluster di backend.

## Caratteristiche tecniche

Il modello architetturale presentato nella sezione precedente ha varie modalità di implementazione: di seguito vengono presentate le caratteristiche tecniche della soluzione. Si sottolinea come queste scelte, soprattutto quelle trasversali, rappresentino un perimetro di riferimento e in generale non un vincolo nell'adozione di soluzioni differenti dovute a scenari di deployment specifici.

### Dettagli Tecnologici

In questa sezione verranno forniti dettagli sulle scelte tecnologiche effettuate in fase di realizzazione.

#### Soluzioni Trasversali

- come IAM viene utilizzato Keycloak;
- come sistema di containerizzazione è utilizzato Docker;
- per l'orchestrazione dei container è stato scelto Kubernetes.

#### Gestione Documentale e Protocollo

- la piattaforma tecnologica è Java;
- per la persistenza la soluzione è compatibile con i database relazionali PostgreSQL, Oracle e MS SQL Server;
- l'application server è WildFly;
- I servizi di back-end sono sviluppati tramite EJB;
- i servizi di front-end sono erogati tramite API Rest;
- i bundle di UI sono sviluppati in Angular ed erogati tramite Web Components.

### Protezione dati personali

Il sistema di gestione documentale “SINFONIA – Protocollo”, basato su piattaforma SIMEL2, consente agli amministratori dell'Amministrazione di monitorare e gestire ruoli e autorizzazioni degli accessi, garantisce sistemi automatici di archiviazione, permette la gestione dei log di Sistema, prevede un Sistema di privacy by design e by default adeguato ai sensi della normativa vigente (crittografia dei dati, diritto all'oblio e identificazione della posizione del dato). Il sistema implementa le misure di sicurezza previste dalla Circolare Agid n. 2/2017 del 18 aprile 2017 e garantisce il pieno rispetto di quanto previsto dal Reg. EU 2016/679 (GDPR). Sono gestite utenze nominali con profilatura completa delle funzionalità e dei dati visibili a utenti e gruppi di utenti, sia in relazione ai dati, sia alle funzioni disponibili. L'accesso degli utenti alle funzionalità e ai dati del sistema viene controllato e regolato, sulla base dei diritti e ruoli posseduti, previa identificazione/autorizzazione a seguito di presentazione di credenziali valide. Sono presenti funzionalità di “audit trail”, consultabili da utenti “gestori”, che tracciano le attività e gli accessi degli utenti in particolare viene tenuta traccia della tipologia dell'evento, il riferimento temporale, chi ha fatto l'operazione, da quale postazione e dettagli aggiuntivi come, nel caso di modifica, il valore del dato prima e dopo l'operazione. La soluzione proposta prevede un sistema di gestione delle password in aderenza allo standard previsto dalla legge sulla privacy D.lgs. 196/2003. Il sistema è dotato di opportuni meccanismi per garantire

e salvaguardare l'integrità e la sicurezza dei dati anagrafici in conformità alle disposizioni vigenti in materia. In merito alle autenticazioni, il sistema recepisce le indicazioni previste nella Circolare Agid n.2/2017, come "password history", "password aging", "password delay", complessità password, alert per creazione/variazione ad utenze amministrative, divieto di utilizzo di determinate password o password che prevedano un contenuto non consentito (parti del nome o del login). In ottemperanza al Reg. EU 2016/679, sono presenti le funzionalità necessarie per garantire i diritti previsti come: oblio, rettifica, limitazione in caso di rettifica e portabilità. Sono adottate tecniche atte a: impedire l'identificabilità diretta del soggetto senza l'utilizzo di informazioni aggiuntive, cifrare le copie di backup e effettuare il logging delle attività di operatori e amministratori. Sono definite procedure operative che rispettano i tempi di comunicazione previsti dal GDPR (art.33 e 34) in caso di violazione dei dati.

Il sistema gestisce la tracciabilità delle modifiche a livello infrastrutturale direttamente sui sistemi RDBMS utilizzati. Il logging avviene a livello transazionale offrendo il massimo livello di accuratezza e veridicità.

Il livello di dettaglio può essere configurato fino ad arrivare alla tracciatura delle letture e non solo delle modifiche. Può essere anche alleggerito quando non è necessario tracciare tutto e può essere elevato a livelli di alta verbosità quando è necessario svolgere analisi approfondite d'uso.

I log prodotti sono consultabili direttamente dall'ambiente interattivo, senza necessità di accedere al file system, semplificando così notevolmente le attività degli amministratori di sistema.

La soluzione proposta dispone di meccanismi che consentano il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti in condizioni di sicurezza nel rispetto delle disposizioni relative in essere. Inoltre, dispone di meccanismi di riconoscimento dell'utente che, abbinati a meccanismi di controllo degli accessi e dei permessi, consentano l'accesso al sistema, alle informazioni ed ai documenti solo agli utenti riconosciuti ed in conformità allo specifico profilo di abilitazione. Questo grado di sicurezza è garantito dal sistema di profilazione dell'utente. Il profilo regola: l'accesso, le informazioni esposte e le funzioni applicative disponibili. Il sistema di protezione dei dati è affidato ad un modulo ACL che, mediante una relazione n-aria fra singola informazione, utente/gruppo e permesso autorizza o concede l'utilizzo degli elementi del sistema informativo.

## **Caratteristiche di sicurezza**

Il sistema di gestione documentale "SINFONIA – Protocollo", basato su piattaforma SIMEL2, garantisce i requisiti di riservatezza, autenticità, integrità, disponibilità e non ripudio di dati, documenti e informazioni. È dotata, infatti, di tracciamento e registrazione, a livello di Sistema con log applicativi, delle attività eseguite da tutti gli utenti, compresi gli utenti di amministrazione.

I log sono conservati per il mantenimento dello storico, sia delle azioni svolte dagli utenti che dei documenti prodotti, e sono immutabili e accessibili agli amministratori individuati dell'Amministrazione.

Il sistema consente la gestione dei meccanismi di identificazione degli utenti, di autorizzazione all'accesso e di tutte le fasi di autenticazione (user login), inclusi i processi di autenticazione forte mediante soluzioni in grado di gestire certificati di autenticazione emessi da Enti certificatori legalmente riconosciuti (smart-card, token, ecc..), conformemente alla normativa vigente.

## Accessibilità e usabilità

La UI di “SINFONIA – Protocollo” è progettata per rendere l’esperienza utente semplice ed intuitiva. Tecnicamente lo sviluppo è realizzato tramite tecnologie web standard come HTML5, CSS3 e javascript (ECMAScript 2022) e la struttura della pagina è quella di una applicazione di tipo Single Page Application.

Particolare attenzione viene data al tema dell’accessibilità: l’applicativo è compliant con le specifiche WCAG 2.1 conformemente agli obblighi imposti dalla Legge Stanca e dalla Direttiva europea 2019/882.

L’accessibilità e l’usabilità del sistema fanno parte del processo di sviluppo stesso dell’applicativo: per monitorare e verificare l’accessibilità della piattaforma SIMEL2, su cui si basa “SINFONIA – Protocollo”, come il contrasto dei colori, il testo alternativo e la navigabilità tramite tastiera, vengono infatti utilizzati degli strumenti automatici e in fase di collaudo il software viene testato anche tramite l’utilizzo degli screen reader JAWS e NVDA.

Oltre alla parte tecnica e normativa, l’impegno per mantenere il software accessibile ed usabile prevede delle sessioni periodiche di verifica con associazioni specializzate nei controlli di software fruibile da utenti con disabilità.

## Cooperazione applicativa

Il sistema di gestione documentale “SINFONIA – Protocollo”, basato su piattaforma SIMEL2, include un API Gateway che rende la piattaforma applicativa aperta alle integrazioni e dotata di capacità di orchestrazione verso sistemi esterni. L’implementazione si avvale di infrastrutture open source (es.: Kong). Il sistema è quindi aperto e predisposto all’interazione, mediante WS che permettono l’invocazione funzionale sincrona o asincrona da un applicativo all’altro e complementano le capacità di coordinamento asincrono basate sul workflow manager e le sue procedure event based.

Il sistema adotta protocolli di comunicazione standard web nativi (XML, WebService - SOAP/REST), LDAP, POP, SMTP, SMIME...). Tali tecnologie consentono la comunicazione e l’integrazione con sistemi esterni a “SINFONIA – Protocollo”, e sono personalizzabili tramite un ambiente di sviluppo specifico che fornisce tool, primitive e web services da utilizzare, anche da parte di partner.

Il sistema garantisce inoltre l’interoperabilità tra differenti sistemi di protocollo delle pubbliche amministrazioni come previsto dalle linee guida AgID.

## Manuale utente

Per informazioni dettagliate sul funzionamento dell’applicazione, si prega di consultare l’ultima versione del Manuale Utente, disponibile nel sistema di gestione documentale “SINFONIA – Protocollo” all’indirizzo: <https://sinfonia-protocollo.regione.campania.it>. Sull’area ad accesso controllato [Formazione protocollo](#) sono disponibili materiali formativi ulteriori, redatti da Regione Campania.