PROGETTO "*Firma con IO*" – Approfondimento tecnico

1 Premessa

Il progetto rappresenta un passo avanti nella trasformazione digitale dell'Ente, garantendo efficienza, sicurezza e accessibilità. L'adozione di un'architettura cloud-native per la soluzione proposta e l'integrazione con l'app IO dimostrano come la tecnologia possa semplificare e migliorare le procedure amministrative di un Ente e la relazione tra cittadini e istituzioni.

2 Introduzione

La digitalizzazione dei servizi pubblici rappresenta una delle principali sfide della Pubblica Amministrazione. La necessità di snellire e velocizzare i processi, garantendo al contempo elevati standard di sicurezza, ha spinto verso la ricerca di soluzioni innovative basate su tecnologie avanzate. Il nostro progetto definisce una soluzione che consente di sfruttare appieno la piattaforma di firma elettronica qualificata one shot "Firma con IO" (che si integra a sua volta con l'app IO) e permette a qualunque utente registrato su quest'ultima di firmare documenti digitali in pochi secondi e da qualunque luogo, eliminando l'utilizzo della carta e riducendo drasticamente i tempi di gestione del processo.

3 Il problema

Il processo di firma tradizionale nella Pubblica Amministrazione presenta diverse criticità:

- tempi lunghi, dovuti spesso a procedure ancora di natura analogica che determinano la necessità di presenza fisica;
- costi elevati in termini di tempo ed economici per gestione, stampa, spedizione e archiviazione documentale;
- rischi di natura giuridica e di sicurezza legati ai documenti cartacei;
- difficoltà di apposizione di firme in presenza, soprattutto in contesti decentralizzati, quali quello del Consiglio regionale della Calabria, in cui numerosi collaboratori esterni, distribuiti su tutto il territorio europeo, hanno necessità di firmare documenti (in primis i contratti di collaborazione con l'Ente).

La sfida è quindi quella di individuare un metodo sicuro, veloce e facilmente accessibile per firmare documenti digitali conferendo loro lo stesso valore legare della firma autografa.

4 La soluzione

L'obiettivo principale del progetto è fornire un punto di accesso unico per l'apposizione della firma elettronica qualificata, sfruttando le API esposte dalla piattaforma "Firma con IO" e le funzionalità dell'app IO.

La soluzione applicativa proposta è implementata mediante un'infrastruttura cloud scalabile e sicura, sviluppata secondo il modello *Twelve-Factor App*. Questo approccio consente di ottenere:

- un'architettura altamente scalabile, resiliente e facilmente portabile;
- automazione completa del ciclo di vita dell'applicazione e un conseguente miglioramento della qualità del software;
- elevati standard di sicurezza e compliance.

In particolare, l'innovazione consiste, tra l'altro, nella scelta di un ecosistema tecnologico *cloud-native*, sfruttando le migliori pratiche DevOps e di sicurezza.

Si segnala, infine, una plus di usabilità consistente nella configurazione di template di posizionamento della firma grafica, associati a specifiche tipologie documentali. Eventuali nuovi template possono essere facilmente integrazioni.

5 Tecnologie utilizzate

Il progetto si basa su un'infrastruttura moderna, con un'attenzione particolare a scalabilità, sicurezza e automazione. Le principali soluzioni metodologiche e tecnologiche utilizzate includono:

- **framework Django**, per il backend, con protezioni avanzate contro CSRF, SQL Injection, XSS;
- **Azure App Services**, per l'hosting della soluzione applicativa, automatizzando il deploy della stessa via CI/CD;
- **Azure Key Vault**, per la gestione sicura delle credenziali e degli ulteriori dati riservati di configurazione;
- **autenticazione Entra ID** (Azure Active Directory), per garantire un accesso sicuro con MFA;
- **GitHub Actions per CI/CD**, per la gestione del branching, con trigger automatici per il rilascio dell'applicazione;
- **metodologia Twelve-Factor App**, per la gestione scalabile del software nel cloud;

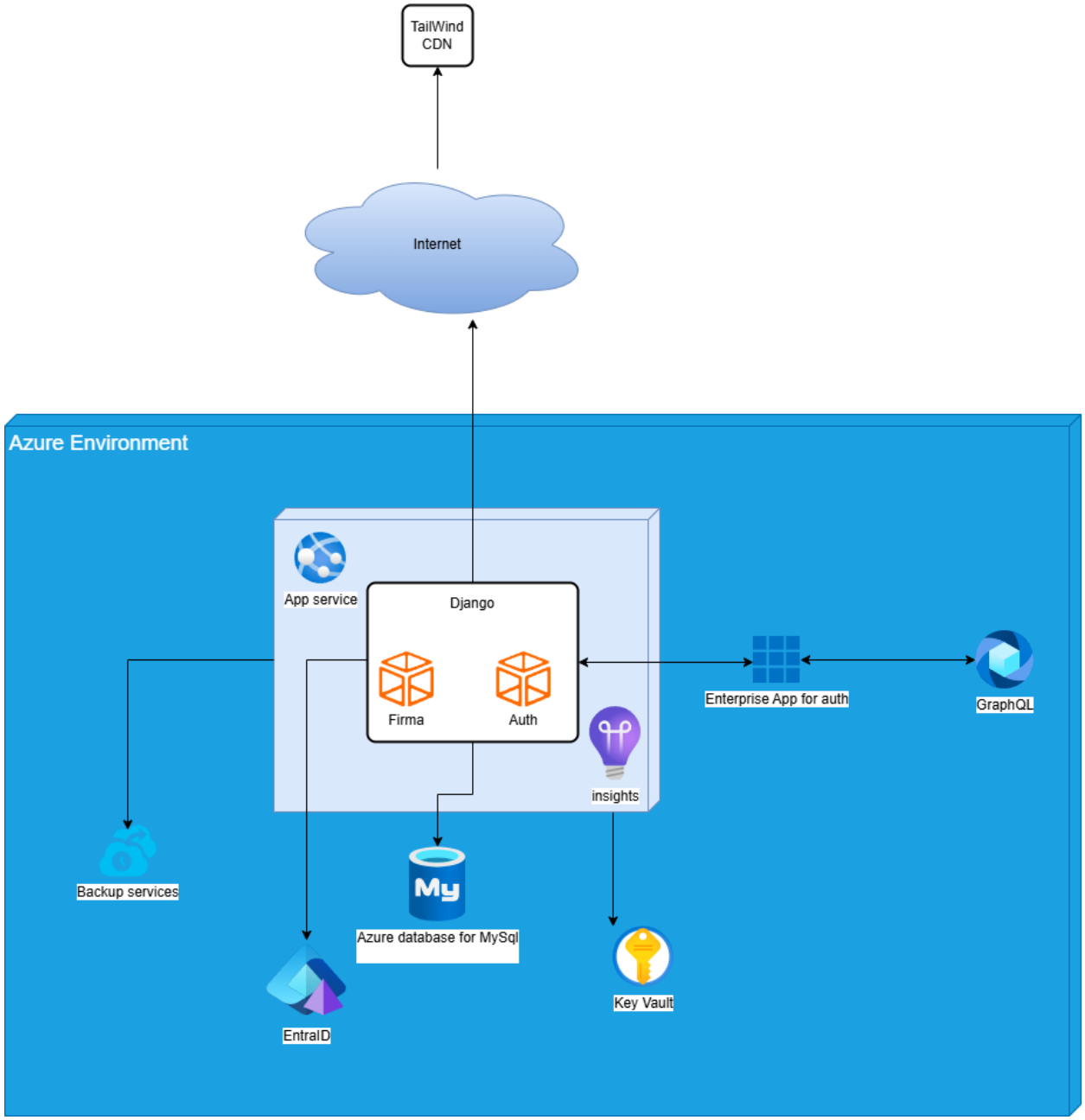
• **containerizzazione** delle componenti dell'applicazione, per una gestione separata (è possibile, per un client esterno, opportunamente autorizzato, accedere agli end-point delle api utilizzate dall'interfaccia grafica), e facilmente manutenibile delle stesse oltre che per sfruttare i vantaggi di portabilità;

• **Azure Database for MySQL**, per la persistenza dei dati della soluzione;

• **GraphQL**, per l'invocazione di servizi di invio automatico di e-mail.

• **backup automatici di Azure**, per garantire continuità operativa e ripristino immediato in caso di guasti.

Di seguito si riporta un diagramma infrastrutturale della soluzione:



5.1 Automazione

Uno dei principali punti di forza del progetto è l'automazione dell'intero ciclo di sviluppo e rilascio. Si segnala soprattutto l'utilizzo delle seguenti soluzioni software e metodologiche:

- **GitHub** e gestione dei branch: ogni nuova feature viene sviluppata in un branch separato, testata e poi unita in produzione;
- **Trigger automatici**: ogni commit su main attiva un workflow GitHub Actions che:
  - esegue i test automatici;
  - crea e pubblica i container Docker su Azure;
  - aggiorna l'applicazione in produzione senza downtime;
- **backup automatici**: tutti i dati e le configurazioni vengono salvati automaticamente tramite le policy di *Azure Backup*, garantendo integrità e ripristino rapido.

Questo approccio garantisce rilasci rapidi, sicuri e senza interruzioni per gli utenti.

L'applicazione della metodologia DevOps consente l'immediata clonazione della soluzione per un eventuale riuso.

5.2 Sicurezza

Il progetto pone una forte enfasi sulla sicurezza, con misure implementate sia a livello di applicazione che di infrastruttura.

L'applicazione è accessibile tramite HTTPS, con protezioni avanzate per la sicurezza degli utenti e dei dati. Sono state implementate misure di sicurezza quali:

- CORS (Cross-Origin Resource Sharing) configurato per limitare l'accesso alle API solo da domini autorizzati.
- CSRF (Cross-Site Request Forgery) Protection, con token di protezione attivi in tutte le richieste che modificano dati sensibili.
- Secure Cookies e SameSite Policies, per prevenire attacchi di session hijacking e cross-site scripting.

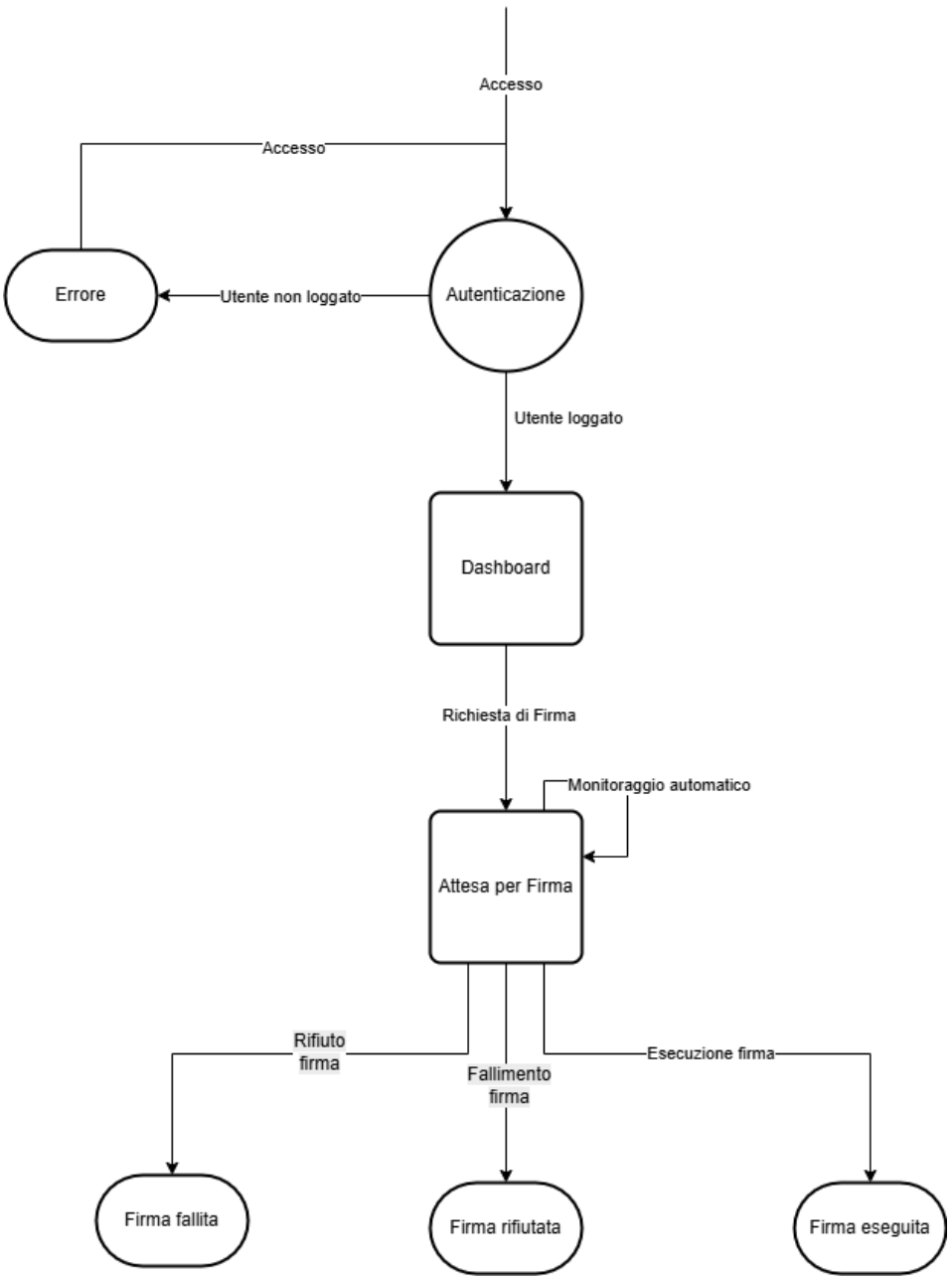
In particolare, si segnalano:

- Sicurezza in ambito **Django**:
  - protezione CSRF e XSS per prevenire attacchi comuni;
  - autenticazione sicura con Entra ID e gestione avanzata delle sessioni.
- Sicurezza in ambito **Azure**:
  - **Azure Key Vault** per la protezione di credenziali e **API keys**;
  - **Azure Web Application Firewall** (WAF) per la mitigazione di attacchi come SQL Injection e XSS.

- accesso limitato ai container tramite firewall e policy di rete;
- monitoraggio continuo con **Azure Security Center**;
- backup automatici per garantire ripristino immediato in caso di guasti o attacchi.

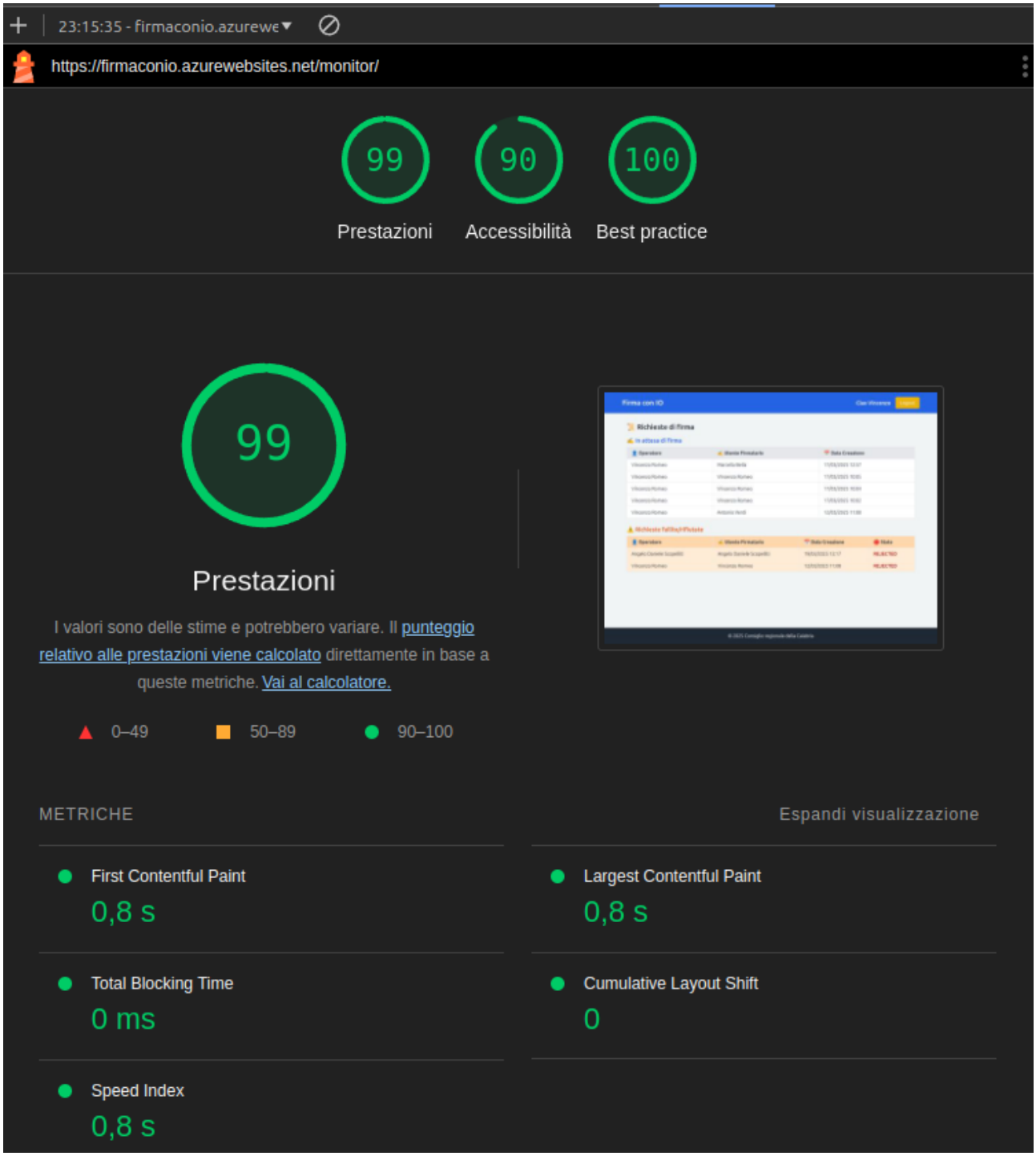
6 Workflow

Si riporta di seguito un diagramma di flusso relativo al processo di firma:



7 Prestazioni e accessibilità

Si riporta di seguito il risultato del test sulle prestazioni e sull'accessibilità della web app effettuato con il tool Lighthouse di Google:



8 Benefici

• Riduzione dei tempi di processo: firma elettronica qualificata apposta in pochi secondi, da qualunque luogo.

• Maggiore sicurezza: eliminazione dei rischi legati a firme cartacee e manomissione documenti.

• Facilità di adozione: accesso centralizzato tramite app IO, già in uso ai cittadini.

• Scalabilità e sostenibilità: modello cloud-native che permette espansione senza impatti operativi.