



PROJECT ORIGIN

projectorigin2023@gmail.com

Specifica Tecnica

Versione	0.1.2
Responsabile	Ibra Elton
Redattori	Andreetto Alessio, Lotto Riccardo
Verificatori	0.1.2
Uso	Esterno
Destinatari	<i>ProjectOrigin</i> Prof. Vardanega Tullio Prof. Cardin Riccardo

Descrizione

Nel presente documento si fornisce una visione approfondita dell'architettura, del design e delle specifiche tecniche del progetto *Personal Identity Wallet*

Registro delle modifiche

Vers.	Data	Autore	Ruolo	Descrizione
0.1.2	2020-09-20	Andreetto Alessio, Lotto Riccardo	Analisti	stesa la struttura definitiva e ampliati tali paragrafi
0.1.1	2023-09-18	Corbu Teodor	Analista	Aggiunte parti Introduzione (capitolo Architettura), Data Scraper, React Material UI
0.1.0	2023-08-25	Andreetto Alessio	Verificatore	Verifica _g del documento
0.0.1	2023-08-24	Corbu Teodor	Analista	Creazione struttura documento, aggiunta Introduzione e spiegazione dei database

Indice

1	Introduzione	3
1.1	Scopo del documento	3
1.2	Scopo del prodotto	3
1.3	Note Esplicative	3
1.4	Riferimenti	3
2	Architettura	5
2.1	Introduzione	5
2.1.1	Container Front-end	5
2.1.2	Container Back-end	5
2.1.3	Container database	5
2.1.4	Container WaltId per standard openID	5
2.1.5	Container di supporto	5
2.2	Componenti Back-end	6
2.2.1	OriginiIssuerApi	6
2.2.2	OriginWalletApi	6
2.3	Componenti Front-end	7
2.3.1	originIssuer	7
2.3.2	originWallet	7
2.3.3	originVerifier	8
2.4	Componenti database	8
2.5	Diagramma delle classi	9
2.6	Design pattern	9
2.6.0.1	Strategy	9
2.6.0.2	Model View-ViewModel	9
3	Elenco dei requisiti	10

Elenco delle figure

Elenco delle tabelle

1 Introduzione

1.1 Scopo del documento

La Specifica Tecnica si pone come obiettivo di descrivere in modo esaustivo l'organizzazione della struttura del software, delle tecnologie adottate e delle scelte architetture compiute dal gruppo durante le fasi di progettazione e di codifica del prodotto.

All'interno del documento si possono trovare gli schemi delle classi per delineare l'architettura e le funzionalità chiave del prodotto, con l'obiettivo di fornire una comprensione completa e chiara del sistema e delle interazioni interne.

Il documento contiene anche una sezione per i requisiti che vengono soddisfatti dal prodotto; questo permette al gruppo di valutare il progresso del lavoro e di tener traccia degli obiettivi imposti.

1.2 Scopo del prodotto

Lo scopo del prodotto è quello di creare una versione semplificata di un applicativo per implementare e rilasciare un "portafoglio di identità digitale" conforme a un insieme di standard, in modo che possa essere utilizzato con qualsiasi servizio, che adotti tale struttura, in qualsiasi paese dell'UE.

In particolare, si dovrà realizzare una web app_g avendo queste componenti architetture:

- Un componente back-office per consentire al dipendente dell'organizzazione emittente di verificare_g manualmente la richiesta di credenziali e autorizzarne l'emissione;
- Un componente di interazione con l'utente dimostrativo per consentire all'utente (titolare) di navigare e richiedere specifiche credenziali da un emittente (ad esempio, il sito di una demo universitaria);
- Un componente di interazione con l'utente dimostrativo per consentire all'utente (titolare) di navigare un sito verificatore_g e fornire le credenziali richieste;
- Un'app front-end per l'utente per archiviare e gestire le proprie credenziali;
- Un componente di comunicazione per consentire lo scambio di credenziali/presentazioni secondo un protocollo standard - il componente di comunicazione sarà implementato tre volte nei tre contesti (lato emittente, lato titolare, lato verificatore).

1.3 Note Esplicative

Alcuni termini utilizzati nel documento possono avere significati ambigui a seconda del contesto. Al fine di evitare equivoci, è stato creato un *Glossario v.1.0.0* contenente tali termini e il loro significato specifico. Per segnalare che un termine è presente nel *Glossario v.1.0.0*, sarà aggiunta una "g" a pedice accanto al termine corrispondente nel testo.

1.4 Riferimenti

1. Normativi:

- *Norme di Progetto v.1.0.0* : contengono le norme e gli strumenti per gli analisti;
- *Capitolato d'appalto C3*: <https://www.math.unipd.it/~tullio/IS-1/2022/Progetto/C3.pdf>;
- *Regolamento del progetto didattico*:: <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/PD02.pdf>.

2. Informativi:

- *Analisi dei Requisiti v1.0.0*;

- **Qualità di prodotto** – slide T8 di Ingegneria del Software: : <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/T08.pdf>;
- **Qualità di processo** – slide T9 di Ingegneria del Software: : <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/T09.pdf>;
- **Verifica e Validazione: introduzione** – slide T10 di Ingegneria del Software:: <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/T10.pdf>;
- **Verifica e Validazione: introduzione** – slide T11 di Ingegneria del Software:: <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/T11.pdf>;
- **Verifica e Validazione: introduzione** – slide T12 di Ingegneria del Software:: <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/T12.pdf>.

2 Architettura

2.1 Introduzione

Per la Realizzazione delle 3 webapp è stata adottata un architettura a microservizi, separando le funzioni di back-end da quelle del front-end. I vari microservizi di ciascuna webapp sono stati sviluppati su container docker differenti.

2.1.1 Container Front-end

- **originIssuer:** È la componete di front-end della webapp Issuer. Essa si interfaccia con l'utente per inviare segnali e ricevere dati dal Back-end *originIssuerApi*. Per la realizzazione del codice è stato adottato il pattern architetturale MVVM (Model-View-ViewModel).
- **originWallet:** È la componete di front-end della webapp Wallet. Essa si interfaccia con l'utente per inviare segnali e ricevere dati dal Back-end *originWalletApi*. Per la realizzazione del codice è stato adottato il pattern architetturale MVVM (Model-View-ViewModel).
- **originVerifier:**È la componete di front-end della webapp Verifier. Essa si interfaccia con l'utente per inviare segnali e ricevere dati dal Back-end *originVerifierApi*. Per la realizzazione del codice è stato adottato il pattern architetturale MVVM (Model-View-ViewModel).

2.1.2 Container Back-end

- **originIssuerApi:** È la componente di back-end della webapp Issuer che si occupa di gestire le richieste provenienti dal front-end e di comunicare con il database *originIssuerDB* per la memorizzazione dei dati.
- **originWalletApi:** È la componente di back-end della webapp Wallet che si occupa di gestire le richieste provenienti dal front-end e di comunicare con il database *originWalletDB* per la memorizzazione dei dati.

2.1.3 Container database

- **originIssuerDB:** È la componente della webapp Issuer che va a eseguire operazioni sul database per la richiesta e la memorizzazione di dati.
- **originWalletDB:** È la componente della webapp Wallet che va a eseguire operazioni sul database per la richiesta e la memorizzazione di dati.

2.1.4 Container WaltId per standard openID

- **openIdIssuer:** È una componente della libreria WaltID per mantenere lo standard openId di comunicazione tra Issuer e le altre webapp, al fine di rispettare le richieste del capitolato.
- **openIdWallet:** È una componente della libreria WaltID per mantenere lo standard openId di comunicazione tra Wallet e le altre webapp, al fine di rispettare le richieste del capitolato.
- **openIdVerifier:**È una componente della libreria WaltID per mantenere lo standard openId di comunicazione tra Verifier e le altre webapp, al fine di rispettare le richieste del capitolato.

2.1.5 Container di supporto

- **adminer:** È un container che permette agli sviluppatori di gestire il database tramite interfaccia web.
- **nginx:** Lo utilizziamo come server proxy per gestire il reindirizzamento del traffico http tramite domini verso i container interni della rete docker

2.2 Componenti Back-end

2.2.1 OriginiIssuerApi

- **authentication:** È una classe che si occupa della autenticazione, ovvero: login, registrazione.
- **datasScraper:** È un insieme di classi che si occupa di dialogare con il database reperendo e memorizzando i dati da esso. È stato realizzato tramite un insieme di 3 classi che rispettano il pattern strategy.
- **openid:** È la classe che si occupa di comunicare con il container openIdIssuer. Essendo le chiamate dipendenti strettamente dallo sviluppo della libreria waltId, il gruppo ha preferito far comunicare il front-end non direttamente con la libreria waltId ma dialogare con questo layer intermedio. In questa maniera il backend si occuperà di fare le chiamate con la libreria waltId del container openIdIssuer.
- **DataResponse:** È una classe che si occupa di parametrizzare il tipo di ritorno che il backend fornisce.
- **InputChecker:** Contiene dei metodi necessari per la verifica e la correttezza degli input fatti al backend.
- **QRCodeGenerator:** È una classe fondamentale nel processo di credential issuing. Vi sono 2 modi per generare una credenziale ovvero: cros device e same device. Questa classe si occupa di generare un qrcode senza generare direttamente l'immagine ma dando via risorsa al frontend lo stream dell'immagine del qrcode tramite il metodo *pipeGenerateQR*.
- **Routing:** In questa classe vengono definite 2 funzionalità principali:
 - Cors ovvero una funzionalità per limitare l'uso da altri dispositivi. Questa opzione viene configurata tramite corsOptions specificando gli indirizzi di origine da cui un utilizzatore potrà usare il backend.
 - Express è una funzionalità che permette di offrire degli endpoint con cui un altro applicativo potrà fare delle chiamate http.

Nel componente vengono configurate le nostre classi precedentemente elencate. Inoltre la classe specifica tutte le chiamate possibili del backend originIssuerApi.

- **index:** Viene creato il routing e il metodo di configurazione degli endpoint.

2.2.2 OriginWalletApi

- **authentication:** È una classe che si occupa della autenticazione, ovvero: login, registrazione.
- **datasScraper:** È un insieme di classi che si occupa di dialogare con il database reperendo e memorizzando i dati da esso. È stato realizzato tramite un insieme di 3 classi che rispettano il pattern strategy. Essendo il database del Walle irrisorio si potrebbe usare un'ulteriore strategia, memorizzando i dati su un file XML o JSON. Questo poiché la struttura dei dati e la complessità è semplice e senza relazioni particolari.
- **openid:** È la classe che si occupa di comunicare con il container openIdWallet. Essendo le chiamate dipendenti strettamente dallo sviluppo della libreria waltId, il gruppo ha preferito far comunicare il front-end non direttamente con la libreria waltId ma dialogare con questo layer intermedio. In questa maniera il backend si occuperà di fare le chiamate con la libreria waltId del container openIdWallet.
- **DataResponse:** È una classe che si occupa di parametrizzare il tipo di ritorno che il backend fornisce.
- **InputChecker:** Contiene dei metodi necessari per la verifica e la correttezza degli input fatti al backend.

- **Routing:** In questa classe vengono definite 2 funzionalità principali:

- Cors ovvero una funzionalità per limitare l'uso da altri dispositivi. Questa opzione viene configurata tramite `corsOptions` specificando gli indirizzi di origine da cui un utilizzatore potrà usare il backend.
- Express è una funzionalità che permette di offrire degli endpoint con cui un altro applicativo potrà fare delle chiamate http.

Nel componente vengono configurate le nostre classi precedentemente elencate. Inoltre la classe specifica tutte le chiamate possibili del backend `originIssuerApi`.

2.3 Componenti Front-end

2.3.1 `originIssuer`

-

2.3.2 `originWallet`

- **App:** questa è la pagina iniziale dell'applicazione, dove viene definito il *routing* delle pagine.
- **components/Navbar:** questa è la componente che definisce la *navbar* dell'applicazione, che differisce dal tipo di utente che è loggato (user, guest, ...).
- **controller/LoginController:** questa è la componente che gestisce la pagina di login dell'applicazione. Esso crea la corrispondente *LoginViewModel* e la corrispondente *LoginView*. Il *controller* si occupa di gestire gli eventi provenienti dalla *view* e di aggiornare la *viewModel*, che a sua volta aggiorna il *model* presente nel back-end.
- **controller/LoginViewModel:** Viene creato dal *controller* ma non ha nessun riferimento ad esso, possiede solo il riferimento al modello dei dati che esso possiede.
- **controller/LoginView:** viene creato dal *controller* ma non ha nessun riferimento ad esso, possiede solo il riferimento al modello dei dati che esso possiede e qualche indicazione di *handling* dei dati.
- **ViewModel:** componente che si occupa del collegamento con il back-end, ha quindi un riferimento al *model*. È unico per tutta l'applicazione

NB. Tutte le componenti seguono la struttura MVVM sopra descritta per la componente *Login*.

- **ListCredential:** componente che si occupa di mostrare la lista delle credenziali dell'utente presenti nel *Wallet*. Da qui si può andare nel dettaglio di una singola credenziale.
- **DetailCredential:** componente che si occupa di mostrare i dettagli di una credenziale presente nel *Wallet*. Da qui si può eliminare una credenziale.

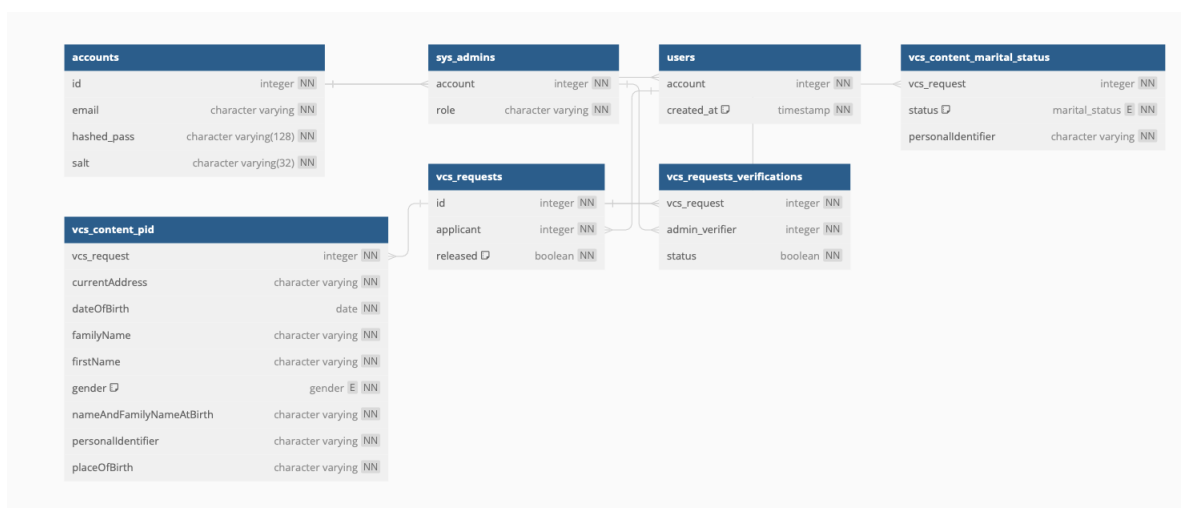
NB. Le seguenti componenti hanno nomi controintuitivi ma sono imposti dallo standard *openID*.

- **InitiateIssuance:** componente che si occupa dell'accettazione di una richiesta di credenziale da parte di un *Issuer* e vengo reindirizzato alla pagina *ListCredential*.
- **CredentialRequest:** Componente che si occupa del re indirizzamento di una richiesta di presentazione di una credenziale parte del *Verifier*.

2.3.3 originVerifier

2.4 Componenti database

- originIssuerDB:



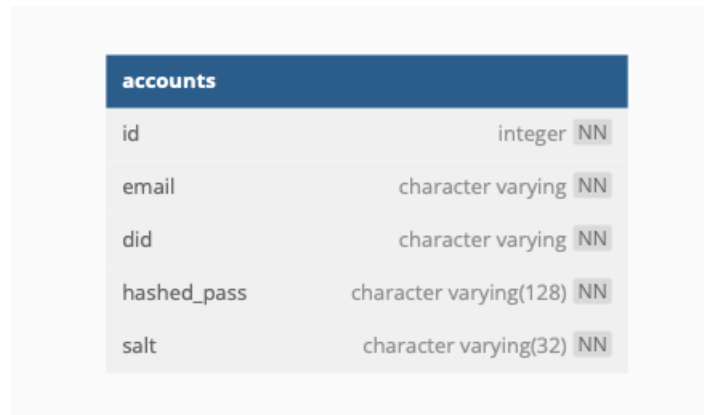
L'immagine sopra riportata descrive il database "issuerdb" implementato mediante un grafico entità-relazioni (schema ER).

Issuerdb è stato pensato per gestire e conservare le informazioni legate agli utenti, alle richieste di certificati digitali (VCS requests) e alle verifiche dei certificati stessi. Per quanto richiesto dal capitolato, e per rispettare la logica dietro tutto il meccanismo dell'Issuer, si distinguono 2 tipi diversi di account: gli account "sys_admins" e gli account "users".

- "sys_admins" sono gli account utilizzati dagli amministratori di sistema, cioè quelle entità che si occupano di approvare (o meglio, verificare) le richieste degli "users" (VCS requests).
- "users", invece, sono gli account utilizzati dai semplici utilizzatori del servizio. Si occupano semplicemente di effettuare delle richieste di certificati di loro interesse alle entità che si occupano di verificare i certificati.

Il contenuto della richiesta approvata e rilasciata può essere di 2 tipi soltanto: un "vcs_content_marital_status" (contenuto riferito allo stato di matrimonio di un utente) o un "vcs_content_pid" (contenuto riferito ad un documento PID di un utente).

- originIssuerDB:



accounts		
id	integer	NN
email	character varying	NN
did	character varying	NN
hashed_pass	character varying(128)	NN
salt	character varying(32)	NN

L'immagine sopra riportata descrive il database “walletdb” implementato mediante un grafico entità-relazioni (schema ER). Walletdb è stato pensato per gestire e conservare (fare lo “storing”) le informazioni legate alle credenziali degli utenti, come espresso da capitolato.

2.5 Diagramma delle classi

2.6 Design pattern

2.6.0.1 Strategy

:

2.6.0.2 Model View-ViewModel

3 Elenco dei requisiti

Requisiti funzionali soddisfatti

Codice	Descrizione	Riferimento	Stato
RF01-O	L'utente inserisce le credenziali nel portale del wallet per iscriversi	UC1	prova
RF02-O	L'utente visualizza un messaggio di errore per dati immessi non corretti, non risulta registrato al wallet	UC4	prova
RF03-O	L'utente può accedere al portale wallet attraverso le credenziali di accesso	UC2	prova
RF04-O	L'utente visualizza un messaggio di errore per credenziali sbagliate al login	UC4	prova
RF05-O	L'utente può eseguire il logout dal portale wallet	UC3	prova
RF06-O	L'utente inserisce le credenziali nel portale Issuer sistema per poter iscriversi	UC5	prova
RF07-O	L'utente visualizza un messaggio di errore durante la registrazione nel portale Issuer sistema per dati immessi non corretti.	UC8	prova
RF08-O	L'utente visualizza un messaggio di errore durante il login nel portale Issuer sistema per dati immessi non corretti.	UC8	prova
RF09-O	L'utente può accedere attraverso le credenziali al portale dell'Issuer sistema	UC6	prova
RF10-O	L'utente può eseguire il logout dal portale dell'Issuer sistema	UC7	prova
RF11-O	L'utente richiede una credenziale PID identificativa nella portale dell'Issuer sistema	UC10	prova
RF12-O	L'utente richiede una credenziale EAA nel portale dell'Issuer sistema	UC11	prova
RF13-O	L'issuer admin effettua il login con le proprie credenziali speciali al portale Issuer sistema	UC6	prova
RF14-O	L'issuer admin accede alla propria dashboard amministrativa	UC6	prova
RF15-O	L'issuer admin esamina la richiesta di credenziale nel portale issuer sistema	UC15	prova
RF16-O	L'issuer admin approva o rifiuta la richiesta di credenziale credenziale portale issuer sistema	UC15	prova
RF17-O	Se la richiesta di credenziale è approvata, l'issuer sistema genera credenziale richiesta	UC15	prova
RF18-O	L'holder può verificare nel portale Issuer sistema lo stato della richiesta credenziale	UC12	prova
RF19-O	Data una richiesta approvata e una credenziale generata l'utente può ottenere nel proprio wallet tale credenziale dal portale issuer sistema	UC14	prova
RF20-O	L'utente ottiene correttamente la credenziale nel proprio wallet	UC14	prova

RF21-O	L'utente visualizza un errore sul wallet che notifica l'errore di rilascio della credenziale	UC13	prova
RF22-O	L'utente visualizza una lista di credenziali memorizzate all'interno del proprio wallet	UC16	prova
RF23-O	L'utente all'interno della propria portale wallet visualizza dettagliatamente la credenziale identificativa PID	UC18	prova
RF24-O	L'utente all'interno della propria portale wallet visualizza dettagliatamente la credenziale identificativa EAA	UC19	prova
RF25-O	L'utente elimina le credenziali memorizzate nel wallet	UC20	prova
RF26-O	Il verifier richiede all'utente una credenziale presente sul wallet personale da verificare	UC21	prova
RF27-O	L'utente fornisce tramite il proprio wallet una credenziale al verifier da verificare	UC22	prova
RF28-O	L'utente riesce a visualizzare un messaggio di errore nella piattaforma verifier che notifica l'errore di verifica	UC23	prova

Numero di requisiti funzionali obbligatori soddisfatti: x/28.