



PROJECT ORIGIN

projectorigin2023@gmail.com

Analisi dei Requisiti

| | |
|---------------------|---|
| Versione | 0.3.2 |
| Responsabile | Ibra Elton |
| Redattori | Beschin Michele |
| Verificatori | |
| Uso | Esterno |
| Destinatari | <i>ProjectOrigin</i> Prof. Vardanega Tullio Prof. Cardin Riccardo |

Descrizione

Questo documento descrive l'analisi dei requisiti del gruppo *ProjectOrigin* nella realizzazione del progetto *Personal Identity Wallet*

Registro delle modifiche

| Vers. | Data | Autore | Ruolo | Descrizione |
|-------|------------|-----------------|--------------|--|
| 0.3.2 | 2023-05-16 | Beschin Michele | Analista | Aggiunti requisiti non funzionali |
| 0.3.1 | 2023-05-16 | Beschin Michele | Analista | Stesura requisiti |
| 0.3.0 | 2023-05-10 | Corbu Teodor | Verificatore | Verifica documento |
| 0.2.1 | 2023-05-10 | Ibra Elton | Analista | Stesura sottocapitoli dei § Casi d'uso |
| 0.2.0 | 2023-05-09 | Corbu Teodor | Verificatore | Verifica documento |
| 0.1.1 | 2023-05-09 | Ibra Elton | Analista | Inizio stesura § Casi d'uso |
| 0.1.0 | 2023-05-04 | Ibra Elton | Verificatore | Verifica documento |
| 0.0.3 | 2023-05-03 | Corbu Teodor | Analista | Stesura § Descrizione Generale |
| 0.0.2 | 2023-05-03 | Corbu Teodor | Analista | Stesura § Introduzione |
| 0.0.1 | 2023-05-02 | Corbu Teodor | Analista | Creazione struttura documento |

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 | Descrizione generale | 4 |
| 2.1 | Obiettivo del prodotto | 4 |
| 2.2 | Funzioni del prodotto | 4 |
| 2.3 | Caratteristiche degli utenti | 4 |
| 3 | Casi d'Uso | 5 |
| 3.1 | Introduzione | 5 |
| 3.2 | Codice identificativo | 5 |
| 3.3 | Attori | 5 |
| 3.4 | Elenco dei casi d'uso | 6 |
| 3.4.1 | UC01 - Richiesta di credenziali per Wallet | 6 |
| 3.4.2 | UC02 - Fornitura delle credenziali per Wallet | 6 |
| 3.4.3 | UC03 - Ottenimento delle credenziali per Wallet | 6 |
| 3.4.4 | UC04 - Visualizzazione delle credenziali | 6 |
| 3.4.5 | UC05 - Cancellazione delle credenziali | 7 |
| 3.4.6 | UC06 - Richiesta credenziali per presentazione | 7 |
| 3.4.7 | UC07 - Fornitura delle credenziali per presentazione | 7 |
| 4 | Requisiti | 8 |
| 4.1 | Introduzione | 8 |
| 4.2 | Elenco dei requisiti | 8 |

1 Introduzione

1.1 Scopo del documento

Il documento si prefigge di esporre e analizzare tutti i requisiti espliciti e impliciti per la realizzazione del progetto Personal Identity Wallet_g, proposto dall'azienda Infocert. Il documento costituirà una base di partenza fondamentale per la fase di progettazione del software, in modo da garantire che essa sia conforme alle richieste fatte dall'azienda proponente Infocert.

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 conforme in qualsiasi paese dell'UE.

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

- 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 contenente tali termini e il loro significato specifico. Per segnalare che un termine è presente nel Glossario, sarà aggiunta una "g" a pedice accanto al termine corrispondente nel testo.

1.4 Riferimenti

1. Normativi:

- **Norme di progetto:** 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>;
- **VE-2023-03-02:** verbale esterno. Primo incontro con Infocert.

2. Informativi:

- **Glossario 0.0.2;**
- **Slide del corso di Ingegneria del Software – Analisi dei Requisiti:** <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/T06.pdf>;
- **Slide del corso di Ingegneria del Software – Diagrammi dei Casi d'Uso:** <https://www.math.unipd.it/~rcardin/swea/2022/Diagrammi%20Use%20Case.pdf>.

2 Descrizione generale

2.1 Obiettivo del prodotto

L'obiettivo del prodotto è quello di permettere all'utilizzatore dell'applicativo (Holder) di raccogliere le proprie credenziali dall'istituzione interessata (Issuer) e di memorizzarle nel loro portafoglio identità. Successivamente le credenziali appena create verranno verificate dalle entità interessate (Verifier) per permettere l'accesso all'Holder all'area interessata. Il Verifier verifica_g le credenziali d'accesso tramite un'infrastruttura chiamata Verifiable Data Registry.

2.2 Funzioni del prodotto

Per quanto riguardano le credenziali d'accesso, dovrà essere possibile:

- Richiedere una credenziale d'accesso;
- Creare e consegnare la credenziale.

Per quanto riguarda l'amministrazione delle credenziali, dovrà essere possibile:

- Vedere le credenziali;
- Eliminare le credenziali.

Per quanto riguarda il Verifier:

- Dovrà richiedere la credenziale;
- L'holder (l'utilizzatore dell'applicativo) dovrà essere capace di consegnare le credenziali appena richieste dal Verifier;
- Il Verifier dovrà validare le credenziali e permettere l'accesso all'utente.

2.3 Caratteristiche degli utenti

L'applicativo potrà essere utilizzato da ogni Holder.

L'Holder potrebbe essere (ma non solo):

- Un'amministrazione pubblica (centrale o locale);
- Un cittadino italiano maggiorenne, oppure un cittadino estero con codice fiscale italiano;
- Un'impresa o un'organizzazione (pubblica o privata);
- Un professionista (avvocato, commercialista, notaio, ecc.);
- Un'università o un centro di ricerca;
- Un'associazione o un'organizzazione no profit;
- Un servizio di pubblica utilità (acqua, gas, energia elettrico, ecc.), finanziario (banca, ecc.), sanitario (Fascicolo Sanitario Elettronico, ecc.), di trasporto pubblico (Trenitalia, ecc.).

3 Casi d'Uso

3.1 Introduzione

In questa sezione sono presentati i casi d'uso che risultano rilevanti per il prodotto Personal Identity Wallet. Essi sono stati individuati e definiti attraverso l'analisi del capitolato d'appalto, gli incontri con il proponente e le riunioni interne del team Project Origin. Ciascun caso d'uso rappresenta un insieme di scenari che hanno lo stesso obiettivo finale per un utente generico del sistema, definito attore. Le norme e le convenzioni adottate per la stesura di ogni caso d'uso sono descritte in dettaglio all'interno del documento Norme di Progetto.

3.2 Codice identificativo

Ciascun caso d'uso viene categorizzato utilizzando la seguente notazione:

CU{XX}. {YY}

Ogni caso d'uso è inoltre definito secondo la seguente struttura:

- ID: il codice del caso d'uso secondo la convenzione specificata precedentemente;
- Nome: specifica il titolo del caso d'uso;
- Attori: indica gli attori principali (ad esempio l'utente generico) e secondari (ad esempio entità di autenticazione esterne) del caso d'uso;
- Descrizione: riporta una breve descrizione del caso d'uso;
- Precondizione: specifica le condizioni che sono identificate come vere prima del verificarsi degli eventi del caso d'uso;
- Postcondizione: specifica le condizioni che sono identificate come vere dopo il verificarsi degli eventi del caso d'uso;
- Scenario principale: rappresenta il flusso degli eventi, a volte attraverso l'uso di una lista numerata, specificando per ciascun evento: titolo, descrizione, attori coinvolti e casi d'uso generati;
- Inclusioni: usate per non descrivere più volte lo stesso flusso di eventi, inserendo il comportamento comune in un caso d'uso a parte;
- Estensioni: descrivono i casi d'uso che non fanno parte del flusso principale degli eventi, allo stesso modo di quanto descritto in "Scenario principale".

Alcuni casi d'uso possono essere associati ad un Diagramma UML dei casi d'uso riportante lo stesso titolo e codice.

3.3 Attori

Attori principali:

- **Holder;**
- **Issuer;**
- **Verifier.**

3.4 Elenco dei casi d'uso

3.4.1 UC01 - Richiesta di credenziali per Wallet

- **Attori:** Holder, Issuer;
- **Descrizione:** Un utente (Holder) deve essere in grado di navigare sul sito dell'emittente (Issuer) e presentare una richiesta per avere una credenziale;
- **Pre-condizione:** L'utente (Holder) deve richiedere delle credenziali;
- **Post-condizione:** L'utente (Holder) è riuscito a presentare la richiesta per le credenziali nel sito dell' Issuer ed ora la sua richiesta deve essere esaminata.
- **Scenario principale:** Credential issuing

3.4.2 UC02 - Fornitura delle credenziali per Wallet

- **Attori:** Issuer, Holder;
- **Descrizione:** Un utente amministratore back-office (Issuer) deve essere in grado di approvare o rifiutare l'emissione di una credenziale per un utente (Holder);
- **Pre-condizione:** L'Issuer deve esaminare ed approvare la richiesta del Holder;
- **Post-condizione:** L'Issuer ha approvato la richiesta del Holder e ha fornito la credenziale. Ora l'Holder ha la possibilità di ottenere la credenziale sul proprio Wallet.
- **Scenario principale:** Credential issuing

3.4.3 UC03 - Ottenimento delle credenziali per Wallet

- **Attori:** Holder, Issuer;
- **Descrizione:** Un utente (Holder) deve essere in grado di ottenere una credenziale sul proprio Wallet;
- **Pre-condizione:** La credenziale è stata approvata e fornita dal Issuer ma l'Holder non è in possesso delle credenziali sul proprio Wallet;
- **Post-condizione:** l'Holder possiede all'interno del proprio Wallet la credenziale.
- **Scenario principale:** Credential issuing

3.4.4 UC04 - Visualizzazione delle credenziali

- **Attori:** Holder;
- **Descrizione:** Un utente (Holder) deve essere in grado di visualizzare l'insieme delle proprie credenziali ricevute sul suo Wallet;
- **Pre-condizione:** L'utente (Holder) non ha ancora visualizzato le credenziali;
- **Post-condizione:** L'utente (Holder) è riuscito a visualizzare le credenziali.
- **Scenario principale:** Credential management

3.4.5 UC05 - Cancellazione delle credenziali

- **Attori:** Holder;
- **Descrizione:** Un utente (Holder) deve essere in grado di rimuovere una credenziale dal proprio Wallet;
- **Pre-condizione:** L'utente (Holder) vuole rimuovere una credenziale dal Wallet personale;
- **Post-condizione:** L'utente (Holder) è riuscito a rimuovere con successo la credenziale dal Wallet personale.
- **Scenario principale:** Credential management

3.4.6 UC06 - Richiesta credenziali per presentazione

- **Attori:** Verifier, Holder;
- **Descrizione:** Un Verifier deve essere in grado di richiedere a un utente (Holder) che sta navigando sul suo sito web di fornire una credenziale (presentazione) che è memorizzata nel Wallet del Holder;
- **Pre-condizione:** Il Verifier vuole richiedere una credenziale al utente (Holder);
- **Post-condizione:** Il Verifier ha presentato una richiesta di una credenziale al utente (Holder) ed ora l'Holder può fornire la propria credenziale.
- **Scenario principale:** Credential consuming

3.4.7 UC07 - Fornitura delle credenziali per presentazione

- **Attori:** Holder, Verifier;
- **Descrizione:** Un utente (Holder) deve essere in grado di fornire al Verifier la credenziale (presentazione) richiesta;
- **Pre-condizione:** L'utente vuole fornire la credenziale presente nel Wallet personale al Verifier;
- **Post-condizione:** La credenziale dell'utente è stata fornita al Verifier.
- **Scenario principale:** Credential consuming

4 Requisiti

4.1 Introduzione

In questa sezione sono elencati i casi d'uso rilevanti per la realizzazione del prodotto Personal Identity Wallet.

4.2 Elenco dei requisiti

Requisiti funzionali

| Codice | Descrizione | Riferimento |
|--------|---|-------------|
| RF01-O | L'utente richiede le credenziali | UC01 |
| RF02-O | L'utente ottiene le credenziali | UC03 |
| RF03-O | L'utente memorizza le credenziali nel wallet _g | UC03 |
| RF04-O | L'utente consuma le credenziali presso un ente | UC07 |
| RF05-O | L'issuer _g fornisce credenziali all'utente | UC02 |
| RF06-O | Un ente chiede all'utente di fornire delle credenziali | UC06 |
| RF07-O | L'utente visualizza le credenziali memorizzate nel wallet | UC04 |
| RF08-O | L'utente elimina le credenziali memorizzate nel wallet | UC05 |

Requisiti non funzionali

| Codice | Descrizione |
|--------|--|
| RN01-O | Le credenziali devono rispettare il formato JSON W3C |
| RN02-O | Le credenziali devono essere scambiate con il protocollo OpenID4VC tra issuer e holder |
| RN03-O | Le credenziali devono essere scambiate con il protocollo OpenID4VP tra holder e verifier |
| RN04-O | Le credenziali possono essere consumate solo dall'effettivo holder |
| RN05-O | Le credenziali non possono essere modificate |
| RN06-O | Le credenziali non possono essere intercettate |