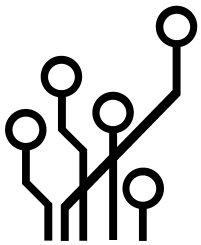

PROJECT ORIGIN

projectorigin2023@gmail.com

Analisi dei Requisiti

Versione	0.3.0
Responsabile	Beschin Michele
Redattori	Ibra Elton
Verificatori	Corbu Teodor Mihail
Uso	Esterno
Destinatari	*ProjectOrigin* 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
0.3.0	2023-05-10	Teodor Corbu	Verificatore	Verifica documento
0.2.1	2023-05-10	Elton Ibra	Analista	Stesura sottocapitoli dei § Casi d'uso
0.2.0	2023-05-09	Teodor Corbu	Verificatore	Verifica documento
0.1.1	2023-05-09	Elton Ibra	Analista	Inizio stesura § Casi d'uso
0.1.0	2023-05-04	Elton Ibra	Verificatore	Verifica documento
0.0.3	2023-05-03	Teodor Corbu	Analista	Stesura § Descrizione Generale
0.0.2	2023-05-03	Teodor Corbu	Analista	Stesura § Introduzione
0.0.1	2023-05-02	Teodor Corbu	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 (documenti personali e certificati) . . . 6
3.4.2 UC02 - Fornitura delle credenziali . . . 6
3.4.3 UC03 - Ottenimento delle credenziali . . . 6
3.4.4 UC04 - Visualizzazione delle credenziali . . . 6
3.4.5 UC05 - Cancellazione delle credenziali . . . 6
3.4.6 UC06 - Richiesta credenziali (presentazione) . . . 6
3.4.7 UC07 - Fornitura delle credenziali (presentazione) . . . 6
3.4.8 UC08 - Validazione credenziali (facoltativo) . . . 7

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:

- **Utente generico:** si riferisce all'utente che non ha ancora eseguito il login al sistema;
- **Utente autenticato:** si riferisce all'utente che ha effettuato il login al sistema;
- **Issuer;**
- **Verifier.**

3.4 Elenco dei casi d'uso

3.4.1 UC01 - Richiesta di credenziali (documenti personali e certificati)

Attori: utente generico;
Descrizione: un utente (Holder) deve essere in grado di navigare sul sito dell'emittente e richiedere una credenziale per il suo portafoglio digitale;
Pre-condizione: l'utente deve richiedere delle credenziali;
Post-condizione: l'utente è riuscito a richiedere le credenziali nel sito dell' Issuer.

3.4.2 UC02 - Fornitura delle credenziali

Attori: utente generico, Issuer;
Descrizione: un utente back-office (lato Issuer) deve essere in grado di emettere una credenziale per un Holder;
Pre-condizione: l'Issuer deve emettere all'utente generico richiedente la credenziale;
Post-condizione: l'Issuer ha fornito la credenziale all'utente generico richiedente. Il richiedente è in possesso della credenziale.

3.4.3 UC03 - Ottenimento delle credenziali

Attori: utente generico;
Descrizione: un utente (Holder) deve essere in grado di ottenere una credenziale dal sito web dell'Issuer;
Pre-condizione: l'utente non è in possesso delle credenziali;
Post-condizione: l'utente possiede all'interno del wallet le credenziali.

3.4.4 UC04 - Visualizzazione delle credenziali

Attori: utente autenticato;
Descrizione: un utente (Holder) deve essere in grado di visualizzare l'insieme delle credenziali ricevute tramite l'applicazione web;
Pre-condizione: l'utente non ha ancora visualizzato le credenziali;
Post-condizione: l'utente è riuscito a visualizzare le credenziali.

3.4.5 UC05 - Cancellazione delle credenziali

Attori: utente autenticato;
Descrizione: un utente (Holder) deve essere in grado di rimuovere una credenziale dall'applicazione web;
Pre-condizione: l'utente vuole rimuovere una credenziale dal wallet personale;
Post-condizione: l'utente è riuscito a rimuovere con successo la credenziale dal wallet personale.

3.4.6 UC06 - Richiesta credenziali (presentazione)

Attori: Verifier, utente generico;
Descrizione: un Verifier deve essere in grado di richiedere a un utente che sta navigando sul suo sito web di fornire una credenziale (presentazione) che è memorizzata nel portafoglio dell'utente;
Pre-condizione: il Verifier vuole richiedere le credenziali dell'utente;
Post-condizione: il Verifier è riuscito ad ottenere le credenziali dell'utente.

3.4.7 UC07 - Fornitura delle credenziali (presentazione)

Attori: utente autenticato, 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 ad un'entità Verifier;
Post-condizione: la credenziale dell'utente è stata fornita al Verifier.

3.4.8 UC08 - Validazione credenziali (facoltativo)

Attori: Verifier;
Descrizione: un Verifier deve essere in grado di validare la correttezza della credenziale (presentazione) ricevuta;
Pre-condizione: il Verifier vuole validare la correttezza della credenziale dell'utente;
Post-condizione: il Verifier è riuscito a validare la correttezza della credenziale dell'utente.