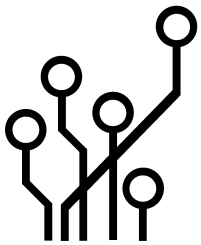

PROJECT ORIGIN

projectorigin2023@gmail.com

Analisi dei Requisiti

Versione	0.1.0
Responsabile	Beschin Michele
Redattori	Corbu Teodor Mihail
Verificatori	Ibra Elton
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
0.1.0	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

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, 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 avendo queste componenti architetturali:

- Un componente back-office per consentire al dipendente dell'organizzazione emittente di verificare 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 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 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.).