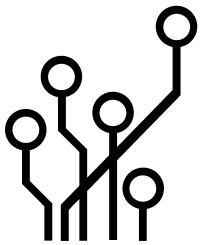


PROJECT ORIGIN

projectorigin2023@gmail.com

Analisi dei Requisiti

Versione	0.6.1
Responsabile	Bobirica Andrei Cristian
Redattori	Andreetto Alessio
Verificatori	
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
0.6.1	2023-07-01	Andreetto Alessio	Analista	Modifica secondo note aziendali
0.6.0	2023-06-05	Corbu Teodor	Verificatore	Verifica documento
0.5.2	2023-06-05	Andreetto Alessio	Analista	Modifica requisiti funzionali
0.5.1	2023-06-04	Corbu Teodor	Analista	Ampliamento parti introduttive
0.5.0	2023-06-03	Ibra Elton	Verificatore	Verifica documento
0.4.1	2023-05-17	Beschin Michele Bobirica Andrei	Analista	Modifica dei casi d'uso
0.4.0	2023-05-17	Lotto Riccardo	Verificatore	Verifica documento
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

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**: Primo incontro con Infocert.
   - **VE-2023-03-22**
   - **VE-2023-05-12**
   - **VE-2023-05-26**
   - **VE-2023-06-09**
2. Informativi:

- **Glossario 0.3.0**;
- **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 creare un'applicazione tramite la quale l'utilizzatore dell'applicazione, l'Holder, riesce a chiedere e successivamente a ricevere le proprie credenziali da un'istituzione (l'Issuer) e a raccoglierle nel suo wallet digitale. Successivamente le potrà gestire ed utilizzare per accedere ad aree riservate che richiedono un metodo di autenticazione. Il Verifier verifica che le credenziali siano integre e valide e permette l'accesso all'Holder all'area riservata richiesta. Per verificare e validare le credenziali il Verifier utilizza un'infrastruttura di supporto chiamata Verifiable Data Registry. Quindi il Verifier interroga il Verifiable Data Registry per controllare la validità delle credenziali fornite dall'Holder. Dopo la verifica delle credenziali d'accesso l'Holder potrà accedere all'area riservata richiesta.

2.2 Funzioni del prodotto

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

- **Creare le credenziali**: l'Holder sarà capace di richiedere le sue credenziali selezionando le informazioni di suo interesse e consegnandole all'Issuer. L'Issuer si impegna di creare la credenziale rispettando i dati forniti dall'utente;
- **Memorizzare e gestire le credenziali**: il Personal Identity Wallet si occuperà di memorizzare tutte le credenziali di accesso dell'utente in un unico luogo digitale sicuro. L'utente potrà visualizzare l'elenco delle credenziali di accesso presenti nel suo wallet;
- **Consegnare in modo sicuro le credenziali**: le credenziali d'accesso create dall'Issuer dovranno essere consegnate in modo sicuro all'Holder. Il Personal Identity Wallet si occuperà di garantire la riservatezza della credenziale; verrà inoltre garantita la possibilità di verifica crittografica da parte di un verifier che la credenziale non sia stata alterata durante la trasmissione.

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

- **Visualizzare le credenziali**: l'Holder sarà capace di visualizzare in modo chiaro e strutturato tutte le proprie credenziali d'accesso disponibili nel suo Personal Identity Wallet con le informazioni di suo interesse (es. Issuer, la data di creazione della credenziale d'accesso e le possibili scadenze);
- **Eliminare le credenziali**: l'utente sarà capace di eliminare le sue credenziali d'accesso che desidera dal proprio Personal Identity Wallet. Questa funzionalità sarà disponibile per garantire la pulizia del wallet ed eliminare le informazioni non più utili.

Per quanto riguarda il Verifier:

- **Richiedere presentazione delle credenziali**: il Verifier dovrà essere capace di richiedere la prresentazione, in modo chiaro e sicuro, delle credenziali d'accesso dell'Holder per permettere l'accesso a determinate aree riservate o a determinati servizi;
- **Consegnare le credenziali richieste**: l'Holder potrà consegnare le credenziali richieste dal Verifier in modo sicuro;
- **Validare le credenziali**: il Verifier verificherà crittograficamente che le credenziali d'accesso fornite dall'Holder siano valide ed integre per poter dare l'accesso ad utenti legittimi e verificati;
- **Concedere l'accesso**: il Verifier, dopo la validazione delle credenziali, dovrà permettere l'accesso all'Holder all'area o ai servizi riservati in modo sicuro.

2.3 Caratteristiche degli utenti

L'applicativo potrà essere utilizzato da ogni attore (Holder, Issuer, Verifier).
I ruoli potrebbero 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 ***holder***. 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{ID} - {Nome}
```

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;
- **Precondizioni**: specifica le condizioni che sono identificate come vere prima del verificarsi degli eventi del caso d'uso;
- **Postcondizioni**: 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;
- **Scenario alternativo**: rappresenta il flusso alternativo degli eventi, a volte attraversdo l'uso di una lista numerata;
- **Estensioni**: usate per estendere i casi d'uso attraverso un aumento delle funzioanalità di essi;
- **Inclusioni**: usate per non descrivere più volte lo stesso flusso di eventi, inserendo il comportamento comune in un caso d'uso a parte.

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

3.3 Attori

- **Holder**: l'Holder è, in generale, un'entità (che può essere un individuo, ma non solo), che potrà gestire le proprie credenziali d'accesso e visualizzarle nel proprio portafoglio digitale. L'Holder utlizzerà questa applicazione richiede credenziali a un issuer e presenta credenziali a un verifier comunicando con gli altri due attori, cioè l'Issuer e il Verifier;
- **Issuer (sistema).**
- **Issuer (Admin).**
- **Verifier**: il Verifier è l'entità che ha lo scopo di richiedere e verificare le credenziali fornite dall'Holder per permettere l'accesso a determinate aree o servizi che richiedono utenti verificati. Il Verifier verifica le credenziali d'accesso dell'Holder utilizzando un'infrastruttura chiamata Verifiable Data Registry;
- **Wallet.**

3.4 Elenco dei casi d'uso

3.4.1 UC1 - Registrazione al Wallet

- **Attore principale:** Holder.
- **Attore secondario**: Wallet.
- **Precondizioni:** L'utente (*holder*) fornisce i seguenti dati per effettuare la registrazione:
  - familyName;
  - firstName;
  - email;
  - password;
  - conferma password.
- **Postcondizioni:** L'utente (*holder*) risulta registrato alla piattaforma del Wallet.
- **Scenario principale:** L'utente (*holder*) ha eseguito con successo la registrazione al sistema web di gestione dei wallet che predispone il wallet ell'utente holder.
- **Scenario alternativo:** L'utente (*holder*) non è riuscito ad eseguire la registrazione per via di:
  - dati immessi non corretti;
  - dati immessi non conformi alle regole di validazione.
- **estensione:** UC4-Visualizzazione Errore.

3.4.2 UC2 - Login al Wallet

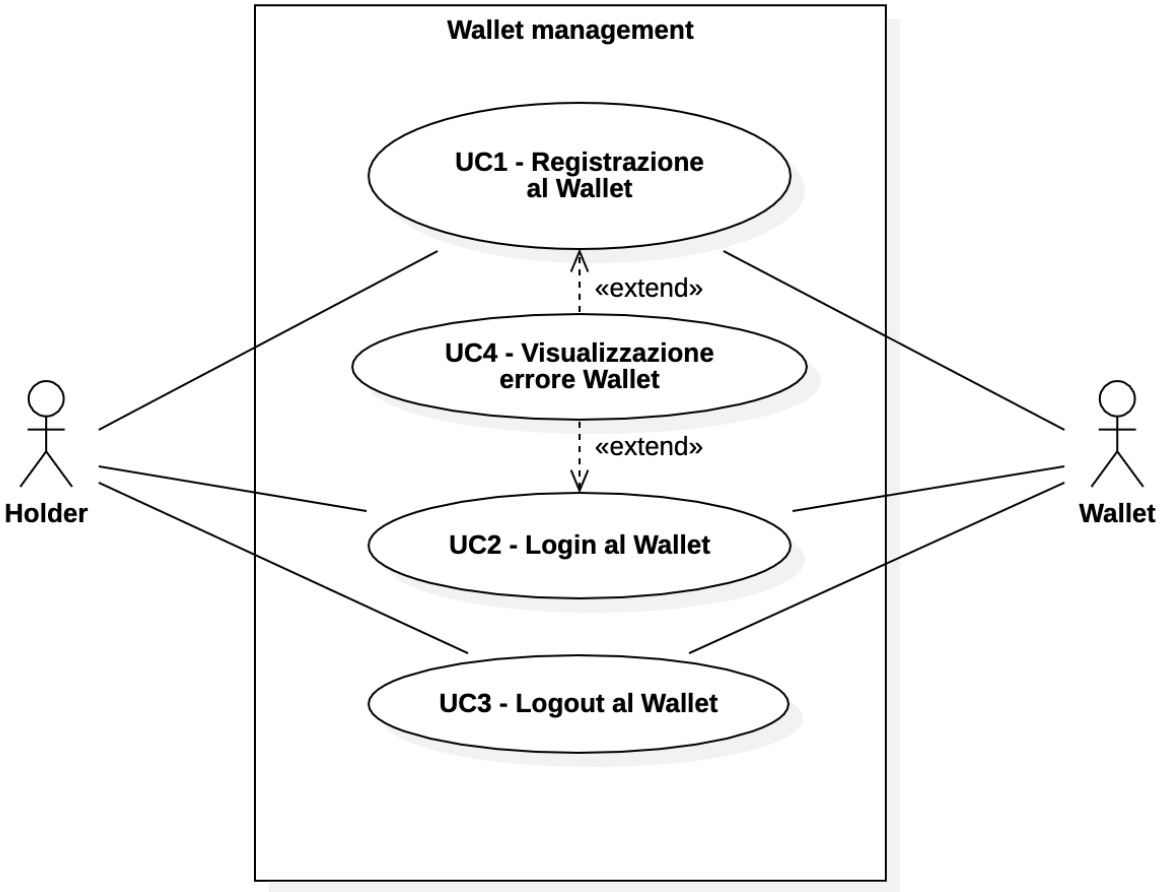
- **Attore principale:** Holder.
- **Attore secondario**: Wallet.
- **Precondizioni:** L'utente (*holder*) che è registrato al sistema deve inserisce le credenziali di accesso ovvero email e password.
- **Postcondizioni:** L'utente (*holder*) una volta inserite le credenziali è riuscito a fare l'accesso al Wallet ed è entrato nel sistema.
- **Scenario principale:** Login è andato a buon fine e l'utente (*holder* si trova all'interno del sistema Wallet.
- **Scenario alternativo**: Login non riuscito, l'utente (*holder*) ha fornito delle credenziali (email e password) non valide.
- **estensione:** UC4-Visualizzazione Errore.

3.4.3 UC3 - Logout dal Wallet

- **Attore principale:** Holder.
- **Attore secondario:** Wallet.
- **Precondizioni:** L'utente (*holder*) vuole effettuare il logout dalla piattaforma Wallet.
- **Postcondizioni:** L' *holder* è uscito dal sistema Wallet e si trova nella schermata di login.
- **Scenario principale:** L'utente (*holder*) è riuscito ad eseguire il logout dal Wallet.

3.4.4 UC4 - Visualizzazione Errore Wallet

- **Attore principale:** Holder.
- **Attore secondario:** Wallet.
- **Precondizioni:** Il caso d'uso da cui estende si trova in una situazione di errore.
- **Postcondizioni:** Viene visualizzato un errore a schermo.
- **Scenario principale:** Viene visualizzato un messaggio d'errore che può riguardare sia il login che la registrazione in base al caso d'uso a cui l'estensione si riferisce.



3.4.5 UC5 - Registrazione all'Issuer sistema

- **Attore principale:** Holder.
- **Attore secondario**: Issuer (sistema).
- **Precondizioni:** L'utente (*holder*) fornisce i seguenti dati per effettuare la registrazione:
  - familyName;
  - firstName;
  - email;

  - password;
  - conferma password.

- **Postcondizioni:** L'utente (*holder*) risulta registrato alla piattaforma dell'Issuer.
- **Scenario principale:** L'utente (*holder*) ha eseguito con successo la registrazione alla piattaforma Issuer.
- **Scenario alternativo:** L'utente (*holder*) non è riuscito ad eseguire la registrazione.
- **estensione:** UC7-Visualizzazione Errore.

3.4.6 UC6 - Login all'Issuer sistema

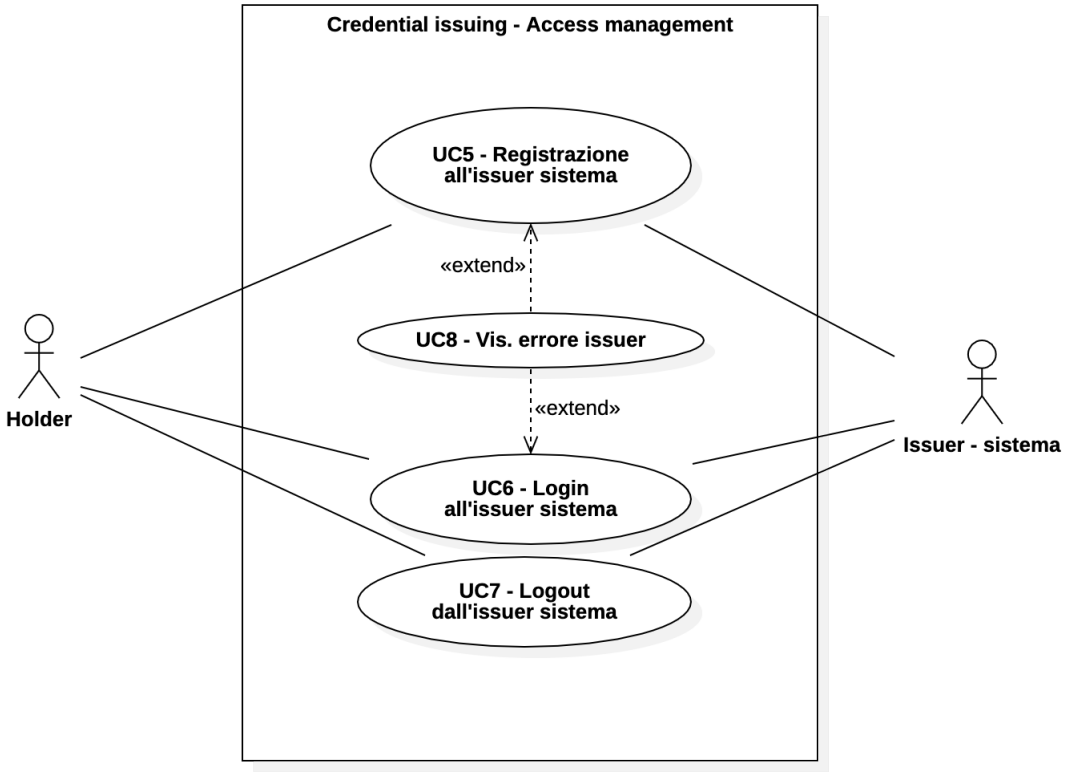
- **Attore principale:** Holder.
- **Attore secondario**: Issuer (sistema).
- **Precondizioni:** L'utente (*holder*) che è registrato al sistema deve inserisce le credenziali di accesso ovvero email e password.
- **Postcondizioni:** L'utente (*holder*) una volta inserite le credenziali è riuscito a fare l'accesso al sistema.
- **Scenario principale:** Login è andato a buon fine e l'utente (*holder* si trova all'interno del sistema Issuer.
- **Scenario alternativo**: Login non riuscito l'utente (*holder*) ha fornito delle credenziali (email e password) non valide.
- **estensione:** UC7-Visualizzazione Errore Issuer.

3.4.7 UC7 - Logout dall'Issuer sistema

- **Attore principale:** Holder.
- **Attore secondario:** Issuer (sistema).
- **Precondizioni:** L'utente (*holder*), che è già loggato alla piattaforma dell'issuer, vuole effettuare il logout dalla piattaforma Issuer.
- **Postcondizioni:** L' *holder* è uscito dal sistema Issuer e si trova nella schermata di login.
- **Scenario principale:** L'utente (*holder*) è riuscito ad eseguire il logout dall'Issuer.

3.4.8 UC8 - Visualizzazione Errore Issuer

- **Attore principale:** Holder.
- **Attore secondario:** Issuer (sistema).
- **Precondizioni:** Il caso d'uso da cui estende si trova in una situazione di errore.
- **Postcondizioni:** Viene visualizzato un errore a schermo.
- **Scenario principale:** Viene visualizzato un messaggio d'errore che può riguardare sia il login che la registrazione in base al caso d'uso a cui l'estensione si riferisce.



3.4.9 UC9 - Richiesta credenziale

- **Attore principale:** Holder.
- **Attore secondario:** Issuer (sistema).
- **Precondizioni:** L' *Holder*, che ha già eseguito il login al sistema di issuer, non è in possesso delle credenziali.
- **Postcondizioni:** L' *Holder* è riuscito a presentare la richiesta per la credenziale nel sito dell'*(*issuer) ed ora la sua richiesta deve essere esaminata.
- **Scenario principale:**
  1. L' *holder* deve richiedere una credenziale;
  2. l' *holder* naviga nel sito dell *issuer*;
  3. l' *holder* presenta una richiesta della credenziale che necessita;
  4. l' *holder* attende che la sua richiesta venga esaminata dall'*Issuer.*
- **Incusioni:**
  - UC9.1- Richiesta PID;
  - UC9.2 - Richiesta EAA;

3.4.10 UC9.1 - Richiesta PID

- **Attore principale:** Holder.
- **Attore secondario:** Issuer (sistema).

- **Precondizioni:** L' *holder* non è in possesso della credenziale identificativa PID, ma ha già eseguito il login nella piattaforma dell'issuer.
- **Postcondizioni:** L' *holder* è riuscito a presentare la richiesta per la credenziale identificativa PID nel sito dell'*Issuer* ed ora la sua richiesta deve essere esaminata.
- **Scenario principale:**
  1. L' *holder* deve richiedere una credenziale PID;
  2. l' *holder* naviga nel sito dell *issuer*;
  3. l'*holder* esegue il login nel portale *Issuer sistema*;
  4. l' *holder* presenta una richiesta della credenziale PID fornendo i seguenti dati:
     - personalId;
     - dateOfBirth;
     - familyname;
     - firstName;
     - gender;
     - nameAndfamilyNameAtBirth;
     - placeOfBirth.
  5. l' *holder* attende che la sua richiesta venga esaminata dall'*Issuer (admin)*

3.4.11 UC9.2 - Richiesta EAA

- **Attore principale:** Holder.
- **Attore secondario:** Issuer (sistema).
- **Precondizioni:** L' *holder* non è in possesso della credenziale EAA, ma ha già eseguito il login nella piattaforma dell'issuer.
- **Postcondizioni:** L' *holder* è riuscito a presentare la richiesta per la credenziale identificativa EAA nel sito dell'*(*issuer) ed ora la sua richiesta deve essere esaminata.
- **Scenario principale:**
  1. L' *holder* deve richiedere una credenziale EAA;
  2. l' *holder* naviga nel sito dell' *issuer*;
  3. l'*holder* esegue il login nel portale *Issuer*;
  4. l' *holder* presenta una richiesta della credenziale EAA fornendo i seguenti dati:
     - personalId;
     - familyName;
     - firstName;
  5. l' *holder* attende che la sua richiesta venga esaminata dall'*Issuer (admin)*

3.4.12 UC10 - Rilascio credenziale

- **Attore principale:** Issuer (admin).
- **Attore secondario:** Issuer (sistema).
- **Precondizioni:** L'issuer non ha ancora verificato la richiesta della credenziale del Holder, la richiesta ha come esito 'In Verifica'.

- **Postcondizioni:** L'issuer ha esaminato la richiesta di rilascio della credenziale del Holder, ora la richiesta ha come esito 'Accettata' oppure 'Rifiutata'.
- **Scenario principale:** La richiesta viene esaminata ed ha come esito 'Accettata'.
- **Scenario alternativo:** La richiesta viene esaminata ed ha come esito 'Rifiutata'.

3.4.13 UC11 - Verifica esito richiesta credenziale

- **Attore principale:** Holder.
- **Attore secondario:** Issuer (sistema).
- **Precondizioni:** L'Holder, che ha eseguito al login all'interno della piattaforma dell'issuer, non ha verificato l'esito della sua richiesta; lo stato della richiesta gli è sconosciuto.
- **Postcondizioni:** L'Holder ha verificato l'esito della sua richiesta, lo stato della richiesta gli è conosciuto.
- **Scenario principale:** l'*Holder* che ha eseguito il login alla piattaforma dell'issuer può visualizzare lo stato della credenziale richiesta: La sua richiesta può avere 3 stati, 'In Verifica', 'Approvata', 'Rifiutata'.

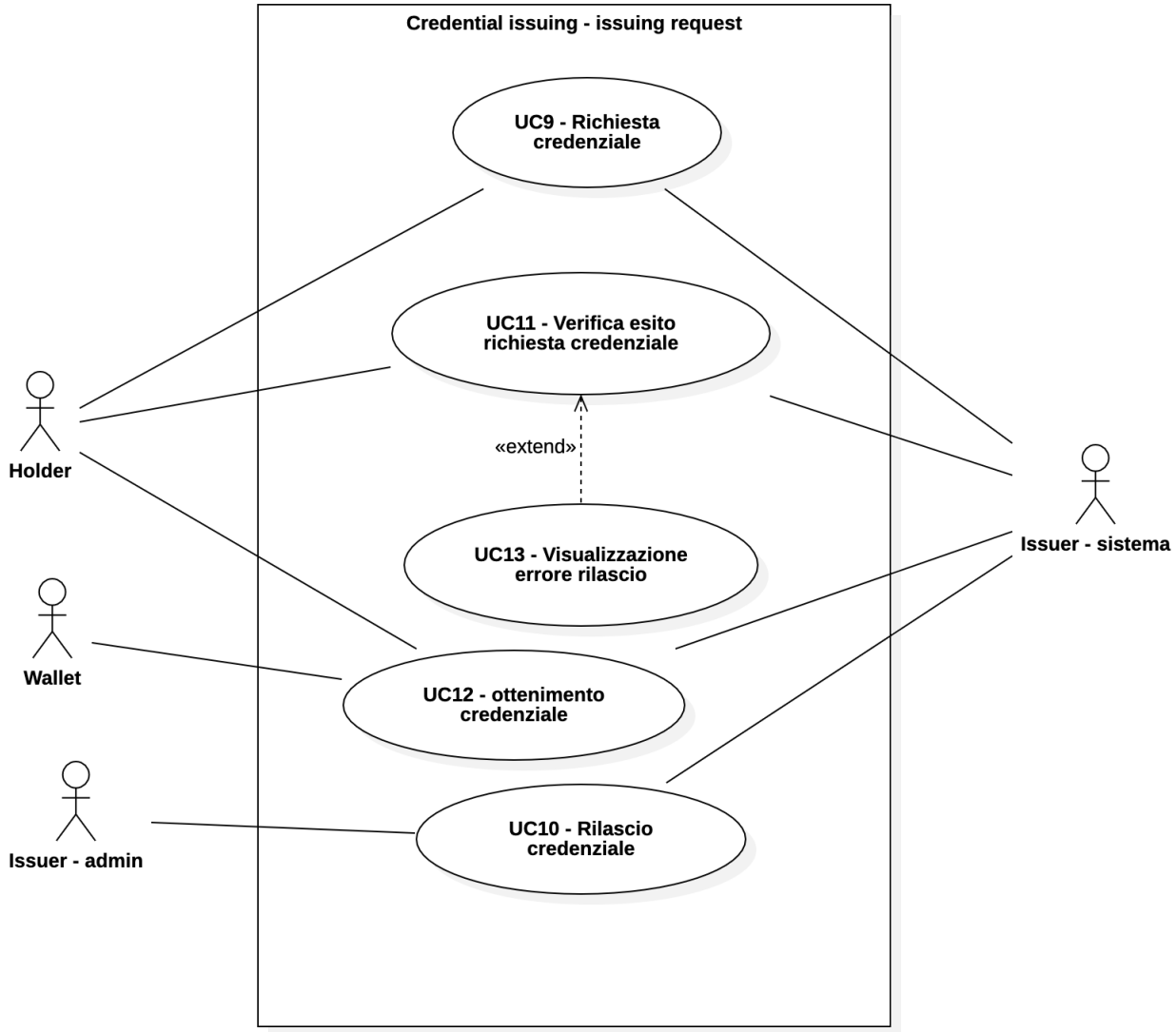
- **Estensioni:**
  - UC13 - Visualizzazione errore rilascio

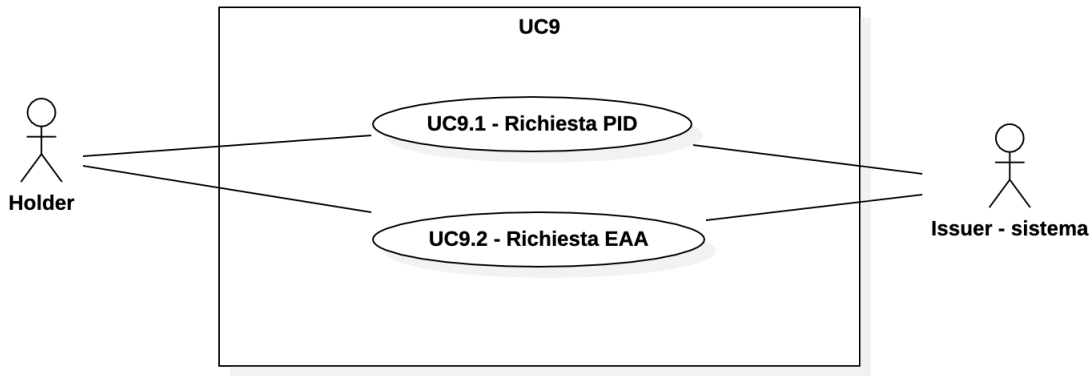
3.4.14 UC12 - Ottenimento credenziale

- **Attore principale:** Holder.
- **Attore secondario:** Issuer (sistema), Wallet.
- **Precondizioni:** L'Holder, che ha eseguito al login all'interno della piattaforma dell'issuer, ha verificato l'esito della sua richiesta, la sua richiesta è stata esaminata e ha come esito 'In Verifica', la credenziale non è all'interno del proprio wallet.
- **Postcondizioni:** L'Holder ha la credenziale all'interno del proprio wallet.
- **Scenario principale:** La richiesta della credenziale ha come esito 'Approvata', L'Holder aggiunge la credenziale sul proprio wallet accetandola.
  La credenziale richiesta è aggiunta al wallet.
- **Scenario alternativo:** La richiesta della credenziale ha come esito 'Rifiutata', l'Holder non può aggiungerla al proprio wallet e la richiesta deve essere rifatta.

3.4.15 UC13 - Visualizzazione errore di rilascio

- **Attore principale:** Holder.
- **Attore secondario:** Issuer (sistema).
- **Precondizioni:** Il caso d'uso da cui estende si trova in una situazione di errore.
- **Postcondizioni:** Viene visualizzato un errore a schermo.
- **Scenario principale:** Viene visualizzato un messaggio d'errore che riguarda il rilascio di una credenziale.


Credential issuing - issuing request
UC9 - Richiesta credenziale
UC11 - Verifica esito richiesta credenziale
«extend»
UC13 - Visualizzazione errore rilascio
UC12 - ottenimento credenziale
UC10 - Rilascio credenziale
Holder
Wallet
Issuer - admin
Issuer - sistema


UC9
UC9.1 - Richiesta PID
UC9.2 - Richiesta EAA
Holder
Issuer - sistema

3.4.16 UC14 - Visualizzazione credenziali

- **Attore principale:** Holder.
- **Attore secondario:** Wallet.
- **Precondizioni:** l'*holder*, dopo aver effettuato il login al Wallet, vuole visualizzare le credenziali presenti nel Wallet.
- **Postcondizioni:** l'*holder* riesce a visualizzare correttamente tutta la lista delle credenziali presenti nel suo wallet.
- **Scenario principale:** Viene visualizzata una lista con tutte le credenziali presenti all'interno del Wallet personale.

3.4.17 UC15 - Visualizzazione singola credenziale

- **Attore principale:** Holder.
- **Attore secondario:** Wallet.
- **Precondizioni:** L' *holder*, dopo aver effettuato il login al Wallet, vuole visualizzare una credenziale dalla lista delle credenziali contenute all'interno del proprio wallet personale.
- **Postcondizioni:** L' *holder* è riuscito a visualizzare la singola credenziale di interesse presente nel wallet personale.
- **Scenario principale:**
- **Incusioni:**
  - UC15.1- Visualizzazione PID;
  - UC15.2 - Visualizzazione EAA;

3.4.18 UC15.1 - visualizzazione PID

- **Attore principale:** Holder.
- **Attore secondario:** Wallet.
- **Precondizioni:** L' *holder*, dopo aver effettuato il login al Wallet, vuole visualizzare la credenziale identificativa PID.
- **Postcondizioni:** L' *holder* visualizza correttamente la credenziale identificativa PID presente nel proprio wallet.
- **Scenario principale:**
  1. L' *holder* vuole visualizzare credenziale PID;
  2. naviga nella lista delle credenziali presente nel proprio Wallet;
  3. una volta scelta la credenziale Pid da visualizzare può consultarla singolarmente in particolare i seguenti campi:
     - id;
     - issuer;
     - issuanceDate (data di richiesta);
     - issued (data di rilascio);
     - validFrom (data di validità);
     - personalId;

  - dateOfBirth;
  - familyname;
  - firstName;
  - gender;
  - nameAndfamilyNameAtBirth;
  - placeOfBirth.

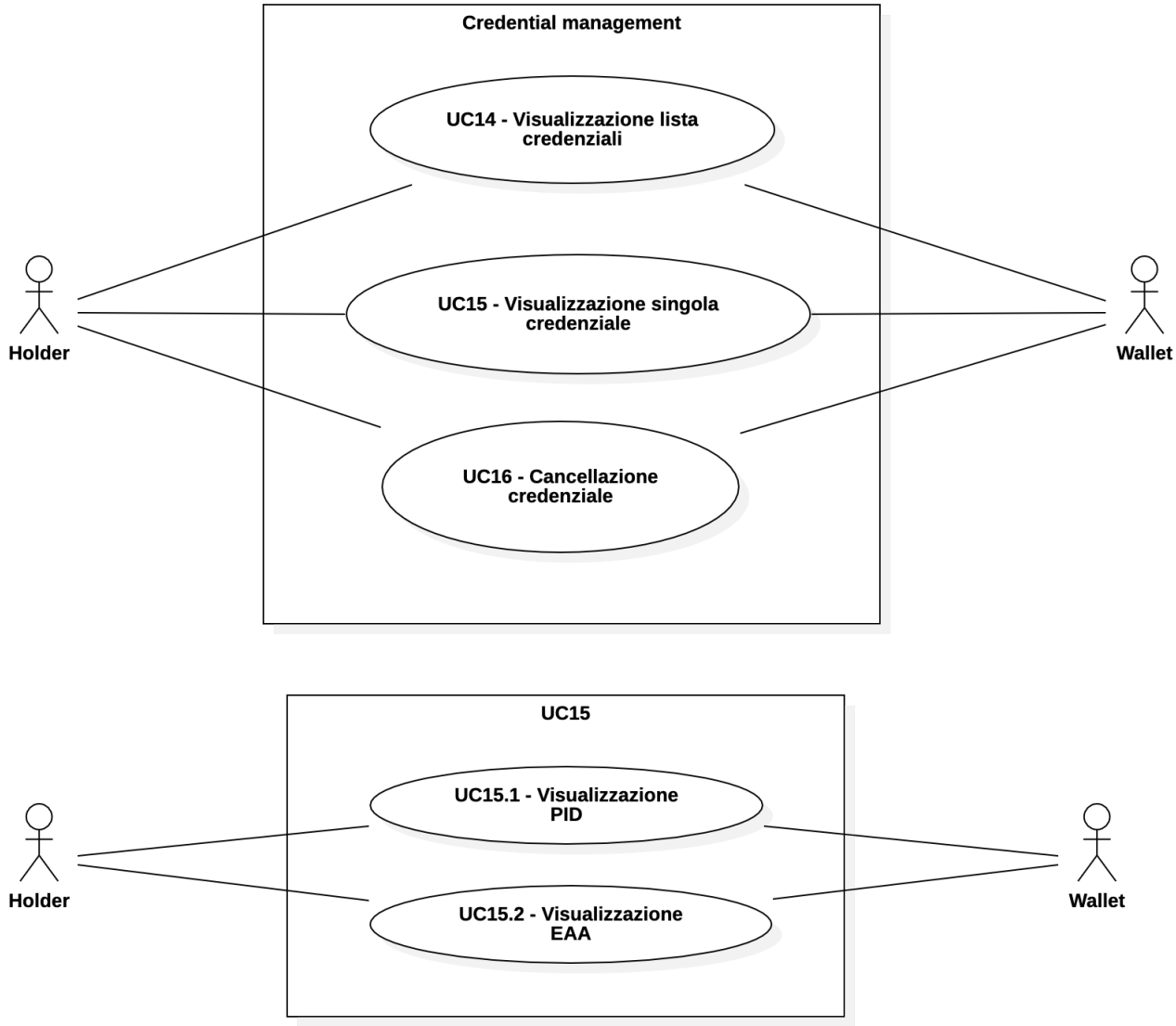
3.4.19 UC15.2 - Visualizzazione EAA

- **Attore principale:** Holder.
- **Attore secondario:** Wallet.
- **Precondizioni:** L' *holder*, dopo aver effettuato il login al Wallet, vuole visualizzare la credenziale EAA.
- **Postcondizioni:** L' *holder* riesce a visualizzare correttamente la credenziale EAA presente all'interno del proprio wallet.
- **Scenario principale:**
  1. L' *holder* vuole visualizzare credenziale EAA;
  2. naviga nella lista delle credenziali presente nel proprio Wallet;
  3. una volta scelta la credenziale Pid da visualizzare può consultarla singolarmente in particolare i seguenti campi:
     - id;
     - issuer;
     - type;
     - issuanceDate (data di richiesta);
     - issued (data di rilascio);
     - validFrom (data di validità);
     - exipirationDate (data di scadenza);
     - status (può essere valido, scaduto, revocato, sospesa);
     - personalId;
     - familyName;
     - firstName;
     - Attributi attestati;

3.4.20 UC16 - Cancellazione credenziale

- **Attore principale:** Holder.
- **Attore secondario:** Wallet.
- **Precondizioni:** L' *holder*, dopo aver effettuato il login al Wallet, vuole rimuovere una credenziale dal suo *Wallet*.
- **Postcondizioni:** L' *holder* ha cancellato la credenziale dal suo *Wallet*.
- **Scenario principale:**
  1. L'*holder* si trova sulla schermata di una crenziale che vuole cancellare;
  2. clicca sul pulsante "elimina";
  3. clicca sul pulsante "conferma";

4. la credenziale è stata cancellata permanentemente.



3.4.21 UC17 - Richiesta credenziali per verifica

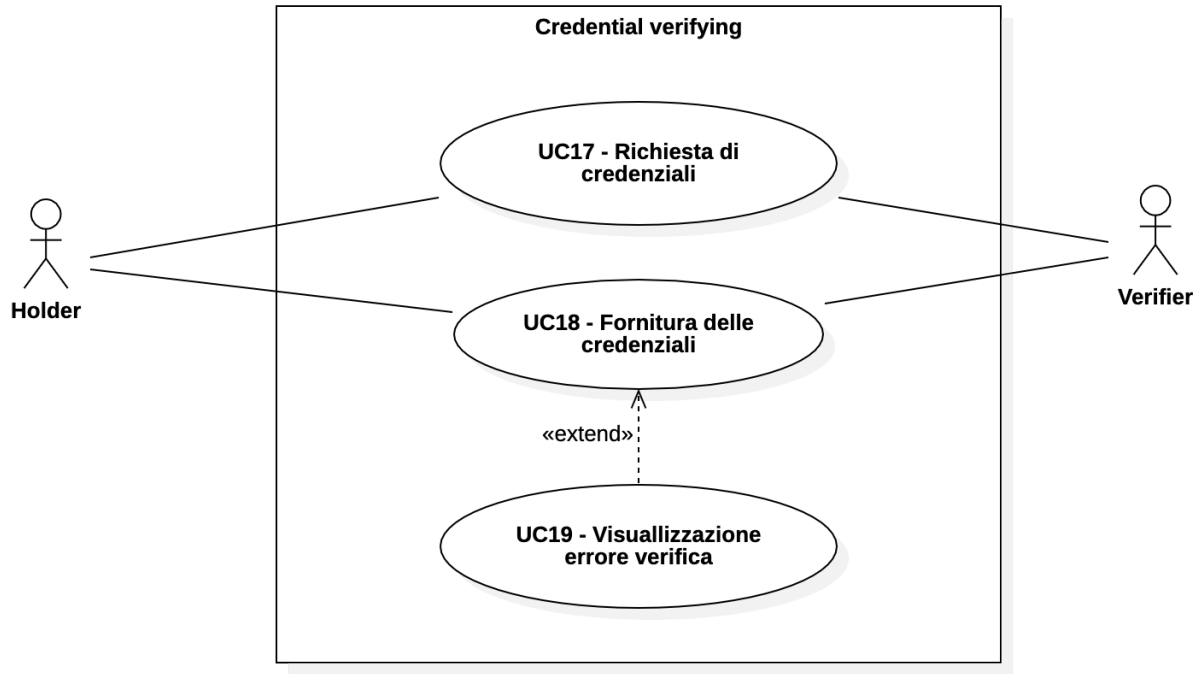
- **Attore principale:** Verifier.
- **Attore secondario:** Holder.
- **Precondizioni:** Il *verifier* deve richiedere una credenziale all' *holder*.
- **Postcondizioni:** Il *verifier* ha presentato una richiesta di una credenziale all' *holder*.
- **Scenario principale:**
  1. Il *verifier* fa richiesta ad un *holder* di fornirgli una credenziale salvata nel suo Wallet.

3.4.22 UC18 - Fornitura delle credenziali per verifica

- **Attore principale:** Holder.
- **Attore secondario:** Verifier.
- **Precondizioni:** L' *holder* vuole fornire la credenziale presente nel Wallet personale al *verifier*.
- **Postcondizioni:** La credenziale dell' *holder* è stata fornita al *verifier*.
- **Scenario principale:** L' *holder* fornisce con successo la credenziale che gli è stata richiesta dal *verifier*.
- **Scenario alternativo:** L' *holder* fornisce delle credenziali non valide e richiama un caso di errore.
- **Estensione:** UC15 - Visualizzazione errore di verifica.

3.4.23 UC19 - Visualizzazione errore di verifica

- **Attore principale:** Holder.
- **Attore secondario:** Verifier.
- **Precondizioni:** Il caso d'uso da cui estende si trova in una situazione di errore.
- **Postcondizioni:** Viene visualizzato un errore a schermo.
- **Scenario principale:** Viene visualizzato un messaggio d'errore che riguarda la fornitura di una credenziale per la verifica.



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 inserisce le credenziali nel portale del wallet per iscriversi	UC1
RF02-O	L'utente visualizza un messaggio di errore per dati immessi non corretti, non risulta registrato al wallet	UC4
RF03-O	L'utente può accedere al portale wallet attraverso le credenziali di accesso	UC2
RF04-O	L'utente visualizza un messaggio di errore per credenziali sbagliate al login	UC4
RF05-O	L'utente può eseguire il logout dal portale wallet	UC3
RF06-O	L'utente inserisce le credenziali nel portale Issuer sistema per poter iscriversi	UC5
RF07-O	L'utente visualizza un messaggio di errore durante la registrazione nel portale Issuer sistema per dati immessi non corretti.	UC8
RF08-O	L'utente visualizza un messaggio di errore durante il login nel portale Issuer sistema per dati immessi non corretti.	UC8
RF09-O	L'utente può accedere attraverso le credenziali al portale dell'Issuer sistema	UC6
RF10-O	L'utente può eseguire il logout dal portale dell'Issuer sistema	UC7
RF11-O	L'utente richiede una credenziale PID identificativa nella portale dell'Issuer sistema	UC9.1
RF12-O	L'utente richiede una credenziale EAA nel portale dell'Issuer sistema	UC9.2
RF13-O	L'issuer admin effettua il lgin con le proprie credenziali speciali al portale Issuer sistema	UC6
RF14-O	L'issuer admin accede alla propria dashboard amministrativa	UC6
RF15-O	L'issuer admin esamina le richiesta di credenziale nel portale issuer sistema	UC10
RF16-O	L'issuer admin approva o rifiuta la richiesta di credenziale credenziale portale issuer sistema	UC10
RF17-O	Se la richiesta di credenziale è approvata, l'issuer sistema genera credenziale richiesta	UC10
RF18-O	L'holder può verificare nel portale Issuer sistema lo stato della richiesta credenziale	UC11
RF19-O	Data una richiesta approvata e una credenziale generata l'utente può ottenere nel proprio wallet tale credenziale dal portale issuer sistema	UC12
RF20-O	L'utente ottiene correttamente la credenziale nel propio wallet	UC12

RF21-O	L'utente visualizza un errore sul wallet che notifica l'errore di rilascio della credenziale	UC13
RF22-O	L'utente visualizza una lista di credenziali memorizzate all'interno del proprio wallet	UC15
RF23-O	L'utente all'interno della propria portale wallet visualizza la credenziale identificativa PID	UC15.1
RF24-O	L'utente all'interno della propria portale wallet visualizza la credenziale identificativa EAA	UC15.2
RF25-O	L'utente elimina le credenziali memorizzate nel wallet	UC16
RF26-O	Il verifier richiede all'utente una credenziale presente sul wallet personale da verificare	UC17
RF27-O	L'utente fornisce tramite il proprio wallet una credenziale al verifier da verificare	UC18
RF28-O	L'utente riesce a visualizzare un messaggio di errore nella piattaforma verifier che notifica l'errore di verifica	UC19

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