



SSI EduWallets

User Manual

SSI EduWallets

User Manual | Call 17 | Project ID 6344

License CC BY-SA

Contents

Introduction.....	3
What are SSI EduWallets?.....	3
What is the purpose of SSI EduWallets?.....	3
What elements does the system consist of?.....	4
Who will take advantage of the implementation?.....	4
Which advantages does the implementation have?.....	5
How does it work?.....	7
Issuance of Verifiable Credentials.....	7
Web wallet issuance flow.....	8
Cross-device issuance flow.....	10
Management of verifiable credentials.....	15
Share verifiable credentials with third parties.....	15
Documental sources.....	17

Introduction

The **SSI EduWallets** project was born with the purpose of transforming the issuance of traditional educational certificates into cryptographically secure and interoperable digital documents called verifiable credentials (VCs), thus eliminating problems such as the forgery of physical documents which are easy to falsify but difficult to verify their authenticity. Adjusting to new web 3.0 standards and the Self-Sovereign Identity (SSI) paradigm through the [European Self-Sovereign Identity Framework \(ESSIF\)](#)¹. This manual describes how to present or request educational verifiable credentials and different user flows implemented within the project.

What are SSI EduWallets?

SSI EduWallets is a software implementation made up of several elements which, once integrated into any e-learning platform, allow the use of self-sovereign identity wallets within these platforms, thus allowing the exchange of verifiable credentials between the user's wallets and the platforms that implement this system.

What is the purpose of SSI EduWallets?

SSI EduWallets allow transforming any traditional e-learning platform to the new self-sovereign identity paradigm of Web 3.0, this allows users to be the owners of their own information so that they are the ones who have full control over how their information is managed, shared, etc. instead of third parties controlling the information.

In addition, this implementation allows the exchange of verifiable credentials between the user's wallets and the platforms, so that users can present certain verifiable credentials to the platforms and the platforms can read them and use that information. The platforms will also be able to issue verifiable credentials that certify that a user has completed certain knowledge at the end of a course or evaluation and these will be stored in the users' wallets to later be used when necessary.

¹ Pastor Matut, C. and Du Seuil, D. (no date) *Understanding the European self-sovereign identity framework (ESSIF)*, PPT. Available at: <https://www.slideshare.net/SSIMeetup/understanding-the-european-selfsovereign-identity-frame-work-essif> (last accessed: 08 July 2023).

The implementation brings the advantages of issuing digital certificates that are secure and can be easily verifiable by third parties and interoperable between other SSI systems.

What elements does the system consist of?

- 1. Wallets:** Wallets are applications that can be installed on a mobile device, or used as a web application, directly from any modern web browser. These wallets work similar to a physical wallet allowing users to store data and share it with third parties. The data that they store are unique identifiers called [Decentralized identifiers \(DIDs\)](#)² and digital credentials called [verifiable credentials \(VCs\)](#)³. Some examples of VCs could be a national ID card or an educational diploma. Any wallet compatible with ESSIF should be compatible with the system.
- 2. Issuer platform:** The platform that implements the SSI EduWallets project can act as an issuer of verifiable educational credentials for its users.
- 3. Verifier platform:** The platform that implements the SSI EduWallets project can act as a verifiable presentation verifier in order to validate, verify and obtain the information of the verifiable credentials that the user is sharing with the platform through their wallet.
- 4. User Interface:** The user interface is the part that is graphically displayed to users on platforms that implement SSI EduWallets. This is in charge of graphically showing users an abstraction of the implementation so that users can easily interact with the platform. The user interface is made up of several graphical components that show the steps of issuing verifiable credentials and presenting verifiable presentations. These graphical components make requests to the different APIs to interact and exchange data.

Who will take advantage of the implementation?

ESSIF wallet users will be able to take advantage of any learning platform that implements the **SSI EduWallets** project whereby they will be able to obtain verifiable credentials in the educational

² Sporny, M. et al. (no date) *Decentralized identifiers (DIDs) v1.0*, W3C. Available at: <https://www.w3.org/TR/did-core/> (last accessed: 08 July 2023).

³ Sporny, M., Longley, D. and Chadwick, D. (no date) *Verifiable credentials data model V1.1*, W3C. Available at: <https://www.w3.org/TR/vc-data-model/#abstract> (last accessed: 08 July 2023).

field upon completion of a course or assessment and will also be able to submit verifiable presentations (VPs) to the platforms to share data with them.

These verifiable credentials will be issued by any learning platform that implements **SSI EduWallets** and they can be stored to the ESSIF wallet of each user. Platforms that implement **SSI EduWallets** can act as issuers to create VCs for the users and verifier to receive and validate the VPs from the users and then leverage this implementation to streamline processes like the verification and validation of a verifiable credential diploma to obtain the knowledge and learning outcomes that a user has acquired.

Which advantages does the implementation have?

The **SSI EduWallets** provide a series of advantages. These advantages are given by the paradigm of SSI (Self Sovereign Identity) in which users are the ones who own their data and not third parties. Users can unify the storage of all their credentials (like the official national identifier or educational diplomas) in a single place, called the "wallet". In this way, users handle directly the information stored in the credentials and they can choose which information they want to share and with whom increasing the user's privacy.

The new paradigm also improves efficiency in tasks such as sending verifiable data to the platforms for verification by eliminating third parties that were in charge of carrying out the verification so that now the recipient is directly in charge of carrying out the verification and then using that information within the platforms, speeding up the process, saving costs and time. Security is built in as the basis of the system ("privacy-by-design") removing certain problems derived from the interoperability, mobility, and forgery.

Following is a brief list of the main advantages of using SSI ESSIF wallets:

- Users own their personal data.
- Unify user information in one place.
- Users choose which data they want to share.
- Streamline platform processes like the presentation of documents.

- Achieve interoperability between different SSI systems that use educational verifiable credentials.
- Issue educational verifiable credentials in a standardized manner following a schema
- Security, the verifiable credentials are secure by Public Key Infrastructure (PKI) encryption, so they're tamper-proof.
- Easy to share skills, competencies, qualifications, or any educational information that a user has attained upon completion of a course or assessment.

The educational verifiable credentials body definition follows the [ELM v3](#)⁴ data model to structure and describe the skills and learning opportunities a user gains by completing a course or assessment. The [ESCO](#)⁵ (European Skills, Competences, Qualifications, and Occupations) is used in conjunction with ELM v3 to classify the learning outcomes of the users and with that information, it is possible to classify the knowledge, learning opportunities, and job occupations.

Educational verifiable credentials are intended to follow and integrate the [Qualification Metadata Schemata \(QMS\)](#)⁶ which documents the skills and qualifications that the person achieves once the course or assessment is completed. The ESCO classification is integrated within the QMS that shows the learning outcomes of the users. With that information it is possible to classify the knowledge, learning opportunities, and job occupations sticking to a cross-country European standard.

⁴ Europass Learning Model *Upcoming launch of the European Learning Model V3: Europass, Upcoming launch of the European Learning Model v3* | Europass. Edited by European Commission. Available at: <https://europa.eu/europass/tr/news/upcoming-launch-european-learning-model-v3> (last accessed: 08 July 2023).

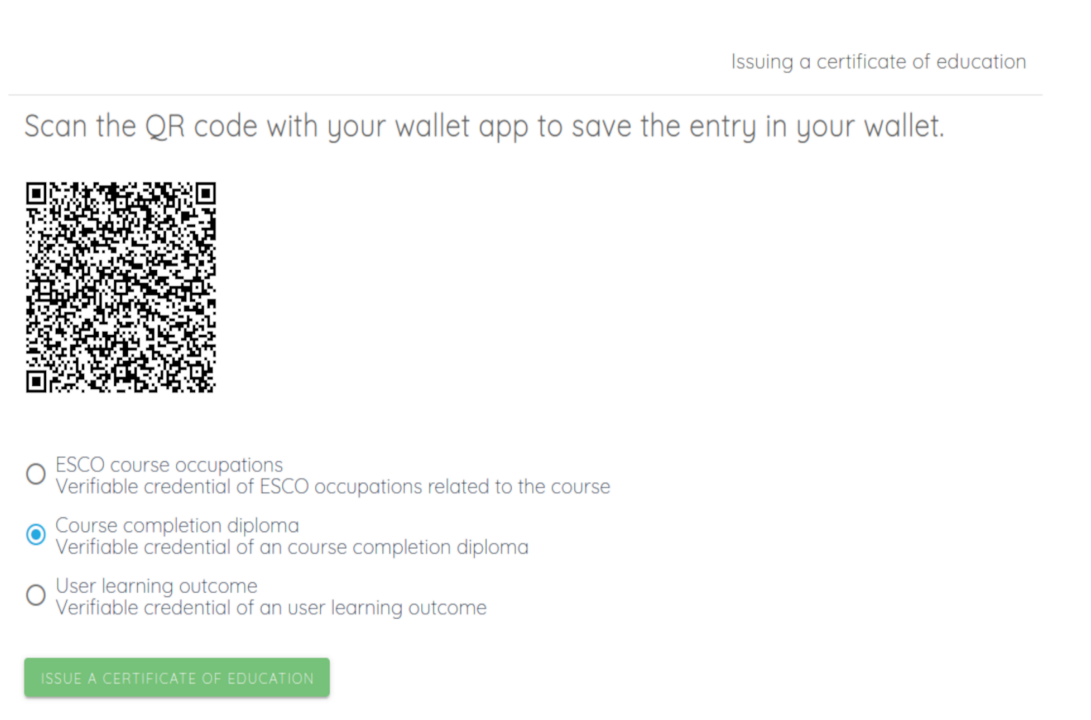
⁵ ESCO *About Esco, ESCO*. Edited by European Commission. Available at: <https://esco.ec.europa.eu/en/about-esco> (last accessed: 08 July 2023).

⁶ European Commission (2020) 'Publishing of Qualification and Learning Opportunity Data Documentation'.

How does it work?

Issuance of Verifiable Credentials

Once the user is authenticated into the platform and accomplishes all the platform requirements to claim a credential the user can choose one of the verifiable credentials available from the issuance portal.



The user can click a button in the user interface to claim the verifiable credential, the button triggers a flow where it calls any ESSIF-compliant wallet that has been preconfigured by the issuer platform. Additionally, the user can scan the QR code generated with any supported ESSIF wallet and triggers the cross-device flow described below.

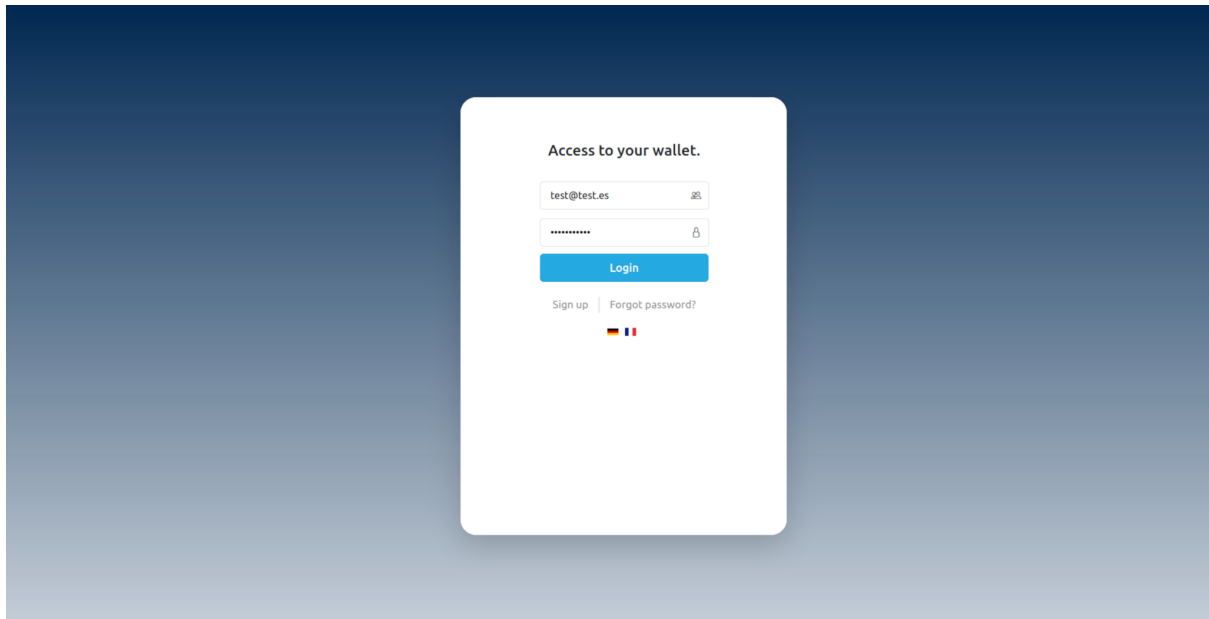
If the user scans the QR code, the cross-device issuance flow will be started. On the other hand, if the user clicks the button, the web wallet issuance flow will be started.

⁷ Issuance portal

Web wallet issuance flow

As a demo web wallet, [Walt.id web wallet](#)⁸ is provided within the project. The login credentials for this demo wallet are not checked, and any email and password will log the user in.

Once the user clicks the button to issue the verifiable credential, he/she is redirected to the wallet where he/she needs to log in (if the user is not logged in already).

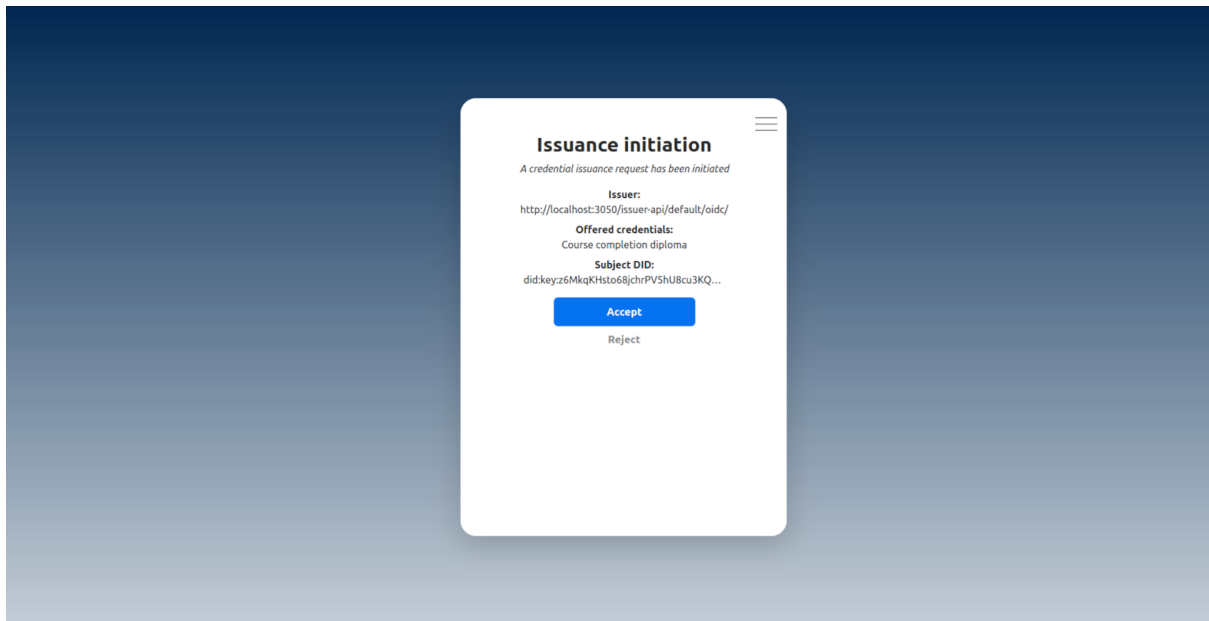


9

Then, the user is prompted to accept or reject the verifiable credential initialization: It is displayed the information about “who-is” the issuer, the VC type, and the subject DID (his/her own identifier). This action will confirm the will of the user to share his personal DID (subject DID) with the issuance portal in order to be included in the VC once created.

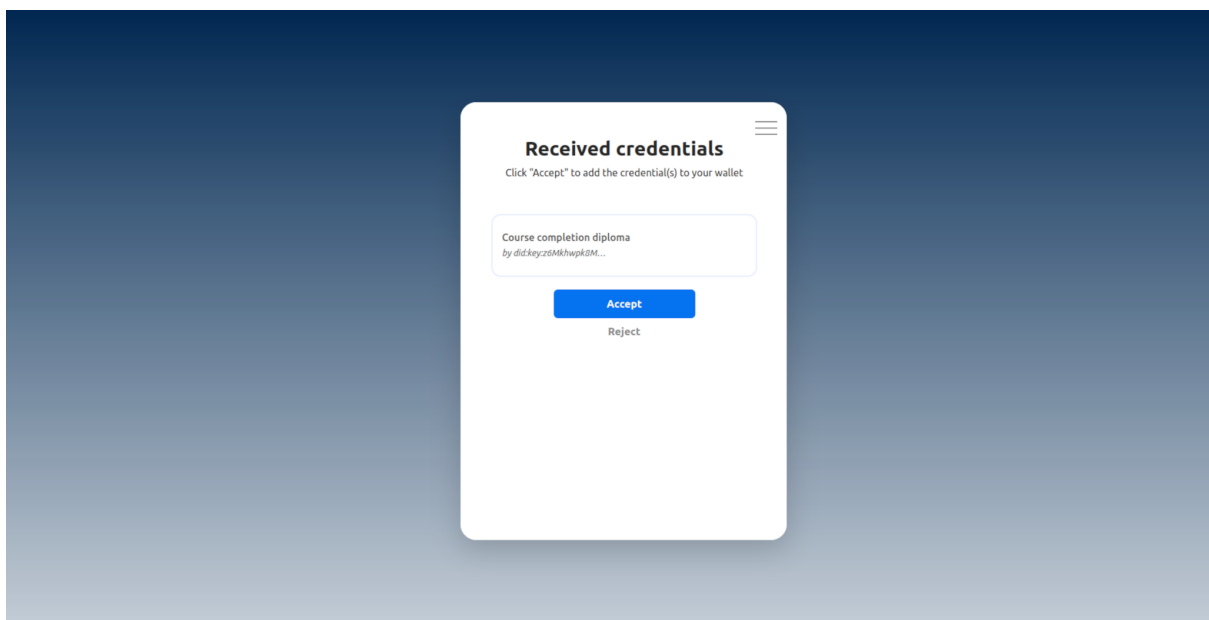
⁸ Walt.id, *Walt.id Web wallet*. Available at: <https://github.com/walt-id/waltid-web-wallet> (last accessed: 08 July 2023).

⁹ Web wallet login



10

Once the user accepts the issuance initiation, then the VC is created and the user can read the data of the VC and accept the storage in the wallet.

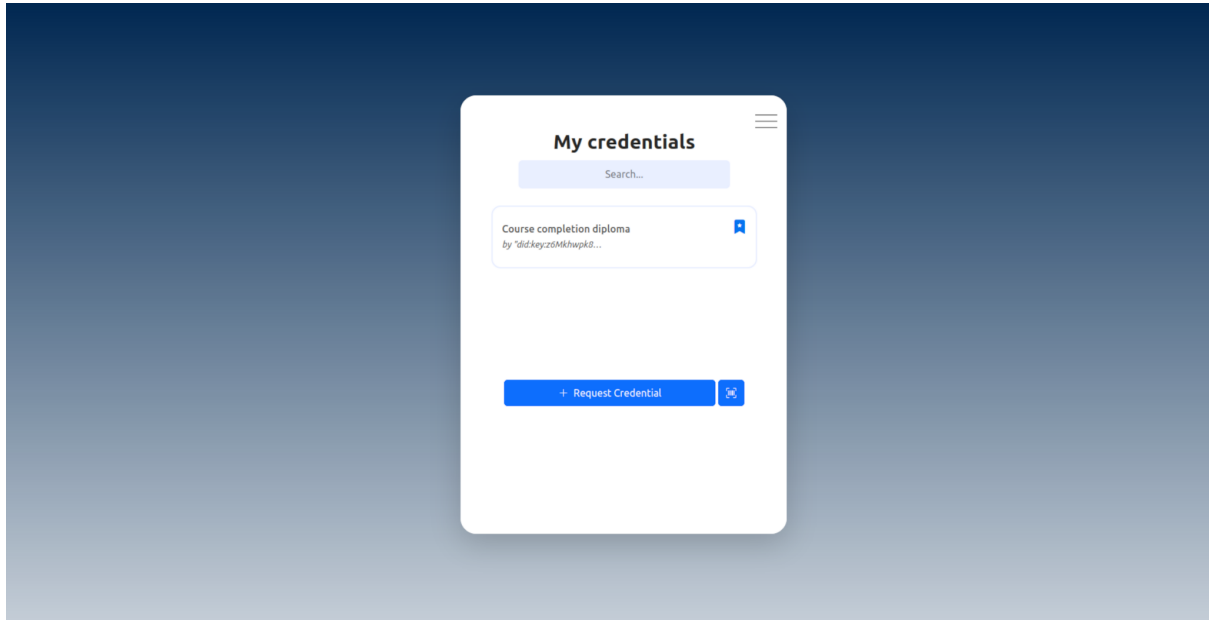


11

¹⁰ Request of issuance notification in the web wallet

¹¹ Web wallet Ui to accept or reject the issued verifiable credential

If the user agrees to receive the verifiable credential, the list of stored credentials held by the user is shown. Once more he could access & read the verifiable credential's data.



12

Cross-device issuance flow

In parallel to the previously described web wallet workflow, the user could decide to use the cross-device flow. Using this workflow has the advantage that any ESSIF-compatible wallet can be used, instead of the wallet pre-configured by the issuer platform.

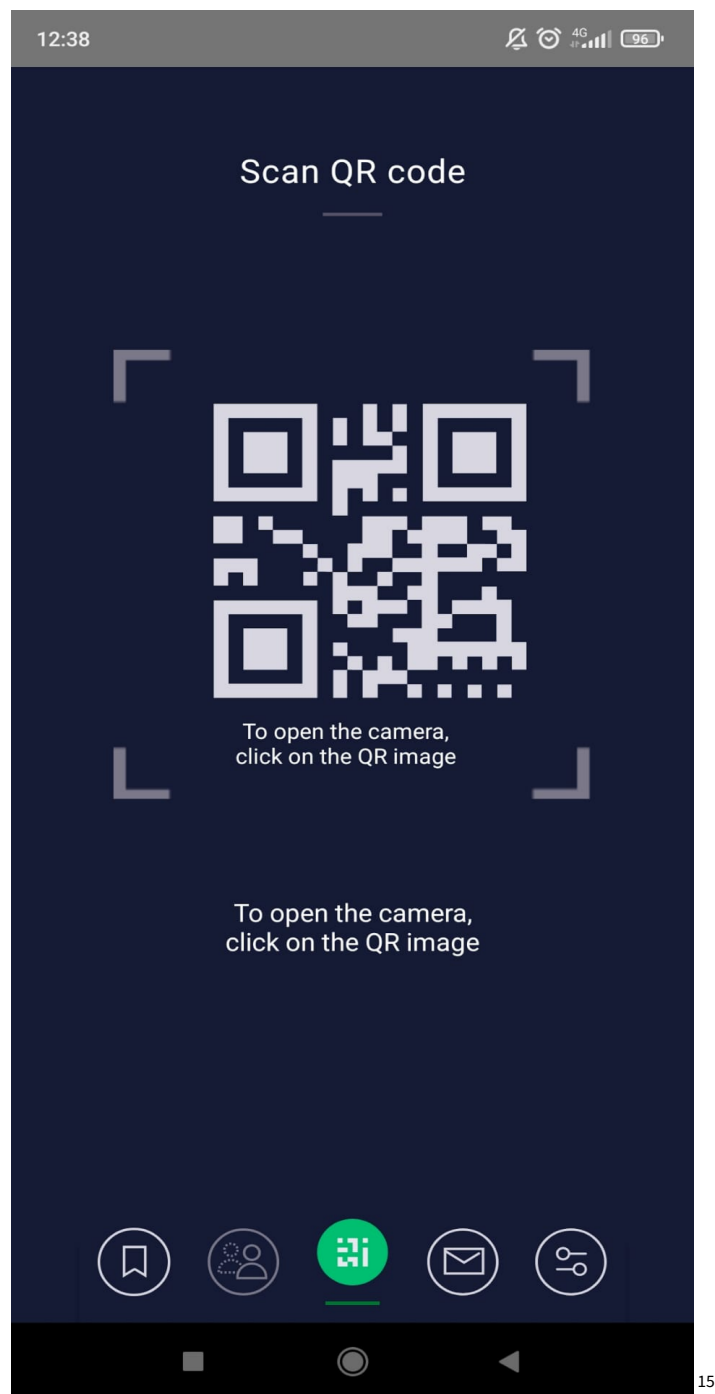
The user will need to open the wallet application. In this demo showcase, we're using the wallet "[ValidatedID](#)¹³", however, any wallet from the list of [ESSIF/EBSI wallets compatibles](#)¹⁴ should be working in a similar way.

¹² Verifiable credentials that the user web wallet has stored

¹³ ValidatedId Validated ID - electronic signature and digital identity providers, Validated ID - Electronic Signature and Digital Identity Providers. Available at: <https://www.validatedid.com/en> (last accessed: 08 July 2023).

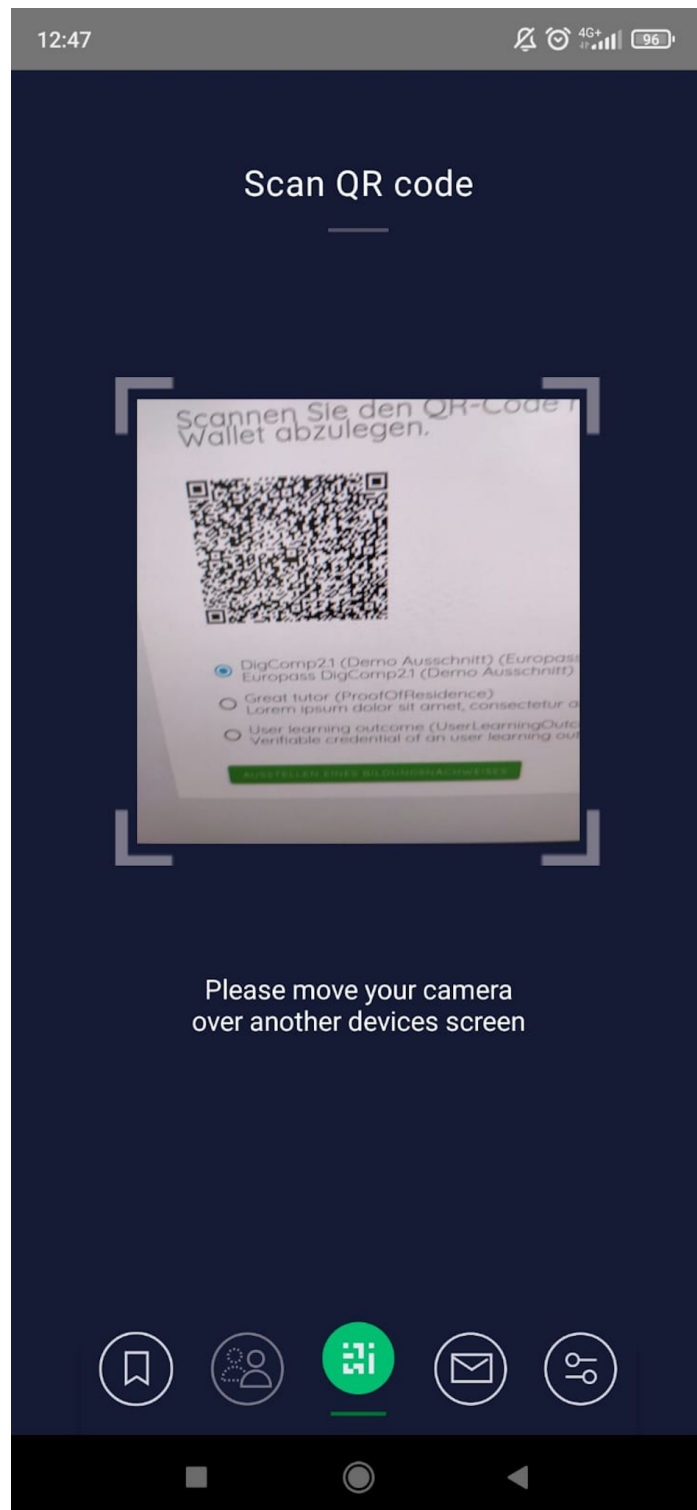
¹⁴ European Commission Conformant wallets, Conformant wallets - EBSI -. Available at: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Conformant+wallets> (last accessed: 08 July 2023).

The user will start the flow by scanning the QR code of the issuer portal using the wallet.



¹⁵ QR scanner of the wallet app

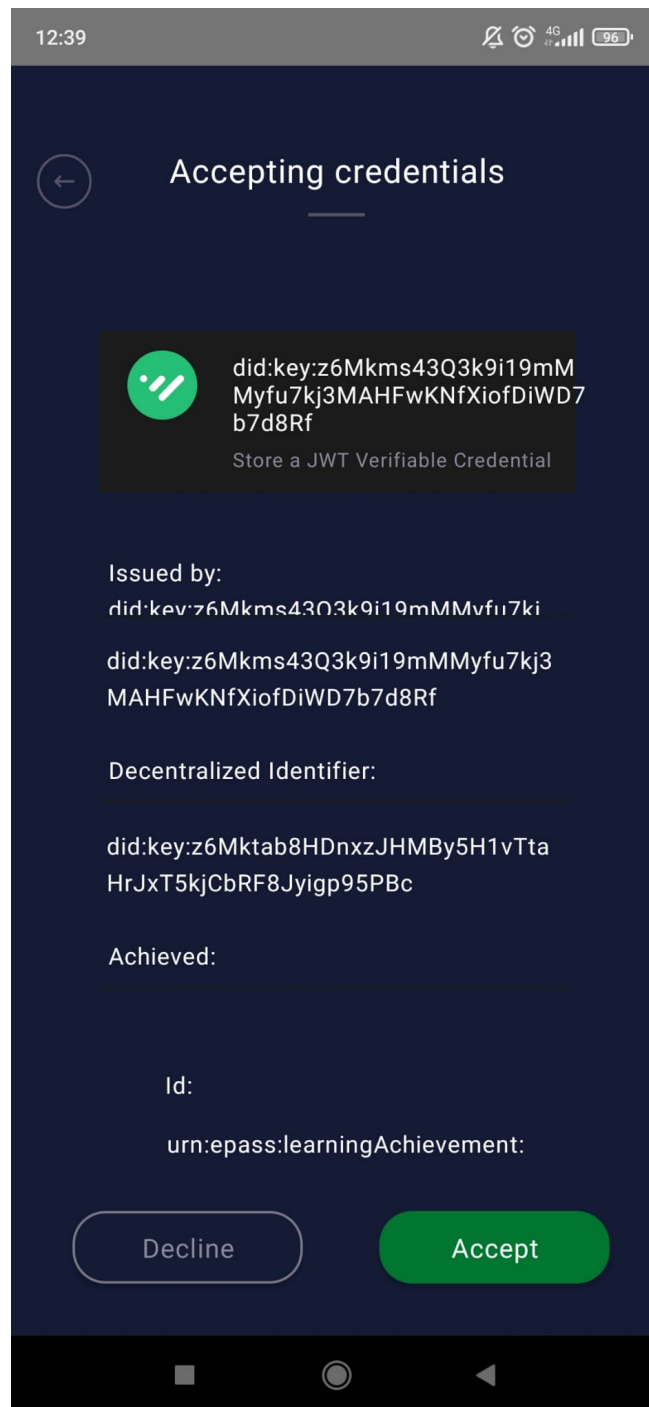
Once the user opens the QR scanner from his wallet, the issuance flow starts and the wallet exchanges data needed to generate the credential (like the DID of the current user using the wallet) automatically with the issuer platform using an HTTPS API connection.



16

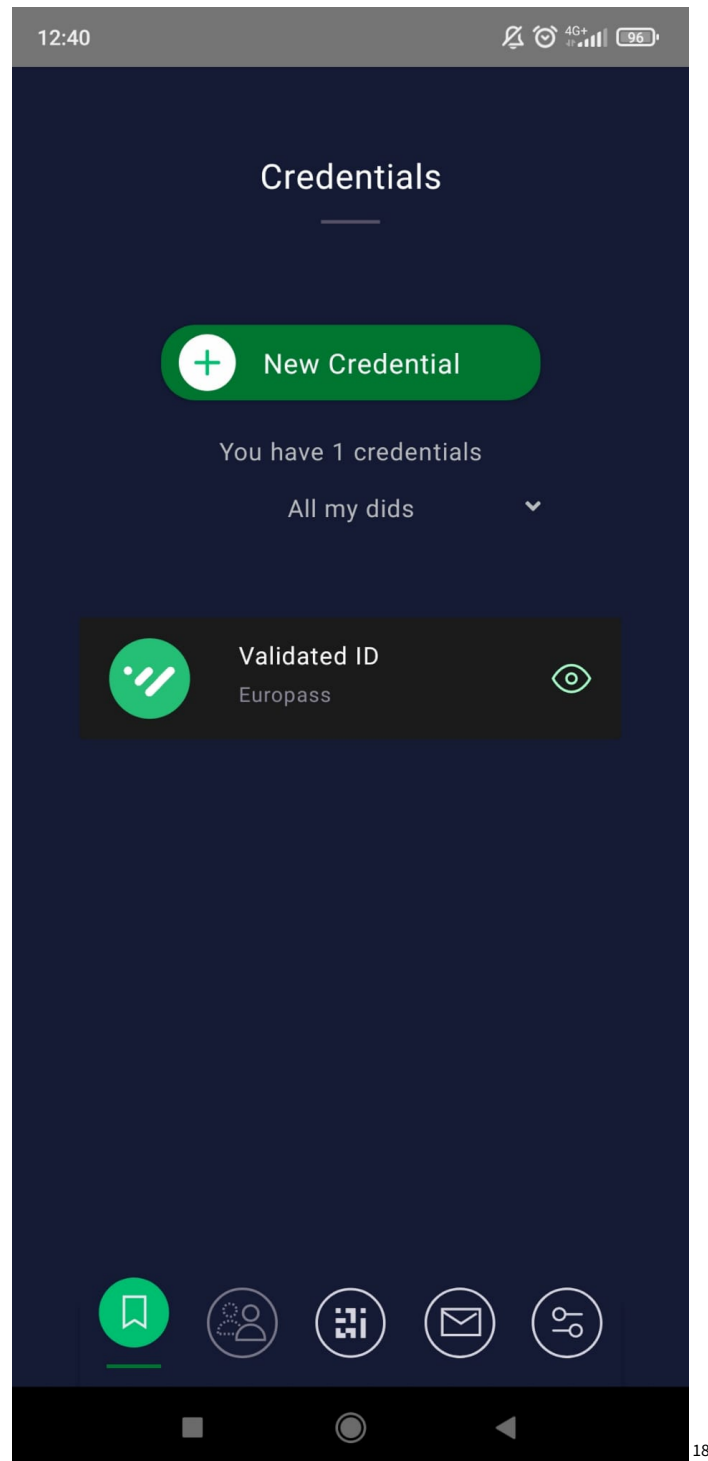
¹⁶ Scanning the verifiable credential to start the issuance process.

Once the issuance flow starts, the issuer sends the verifiable credential to the user's wallet, where the user can review the verifiable credential and check the data contained like identity of the issuer, the DIDs of the issuer and the user himself, and all other fields that describe the verifiable credential itself. The user can accept or reject the issuance of the verifiable credential.



¹⁷ Wallet app UI to accept the verifiable credential or reject it

Once the user accepts the issuance request, the verifiable credential is stored in his wallet and it is displayed in the credentials list. From this list, the user can check the type of verifiable credential and open it to read the information contained.



¹⁸ Wallet app UI listing the Verifiable credentials that the user has

Management of verifiable credentials

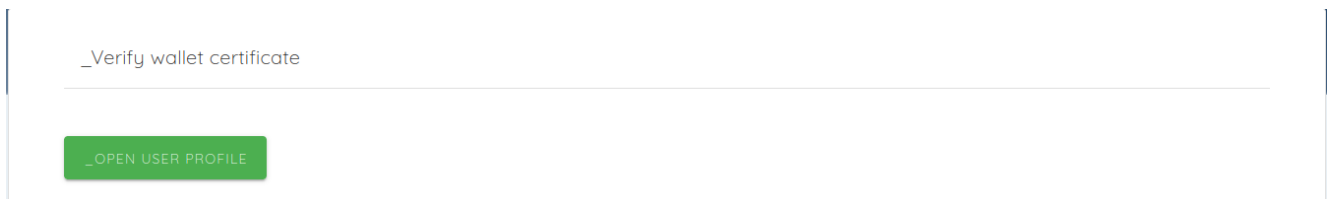
Since the users can use any ESSIF-compliant wallet, the functionality and possibilities may vary between the different wallets. It is the user's choice which wallet application he/she will use. The management of credentials and details of the individual usage of the wallet application is out of the project scope.

The demo wallet provided by the SSI EduWallets project includes the following basic functionalities:

- Accept or reject the issuance of a verifiable credential
- Accept or reject the request for a verifiable presentation
- Receive and store verifiable credentials on the web wallet
- List the content of the verifiable credentials
- Delete the verifiable credentials

Share verifiable credentials with third parties

When a third party needs a user's verifiable credential to carry out an action such as the verification and validation of previous knowledge obtained, the first step is to go to the verification portal UI.

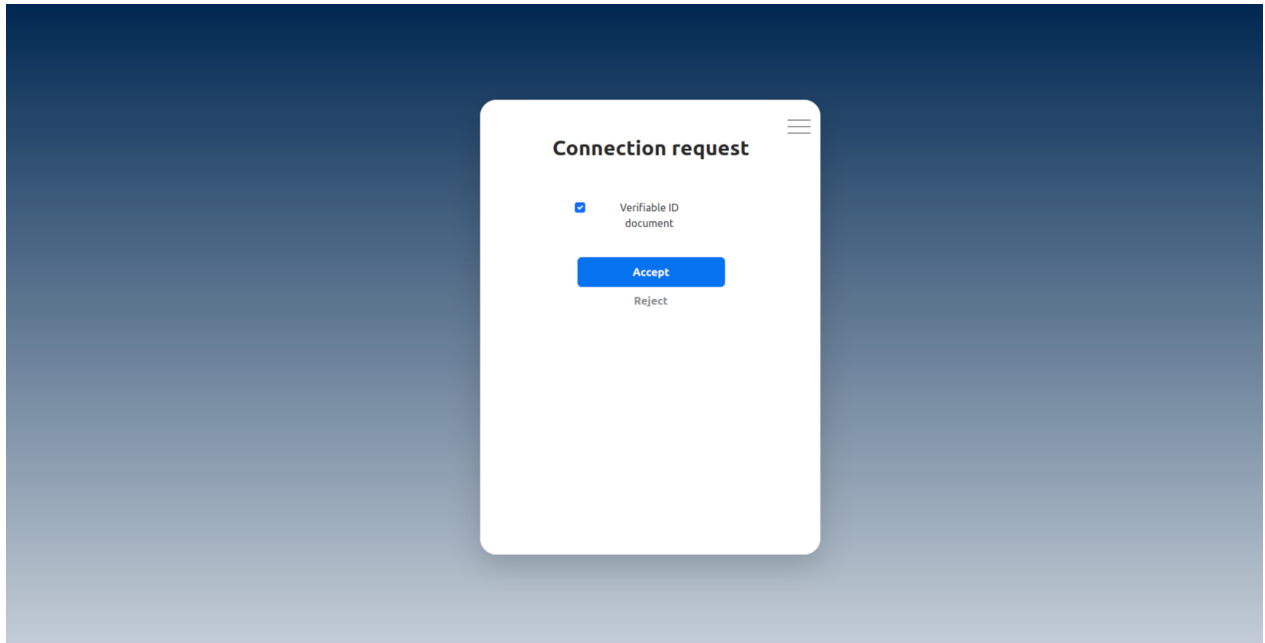
A screenshot of a web interface for a verification portal. It features a light blue header bar with the text "_Verify wallet certificate" in a small, dark font. Below the header is a large, empty white rectangular area. At the bottom left of this area is a green rectangular button with the text "_OPEN USER PROFILE" in white, uppercase letters.

19

From this place, the user can start the verification process and send a VP (verifiable presentation) to the platform.

After the user clicks on the button to start the verification process, an HTTPS request is sent to the user's wallet asking for a specific type of verifiable credential to be shared. After this, the user is required to select and share the specified verifiable credential with the third-party platform.

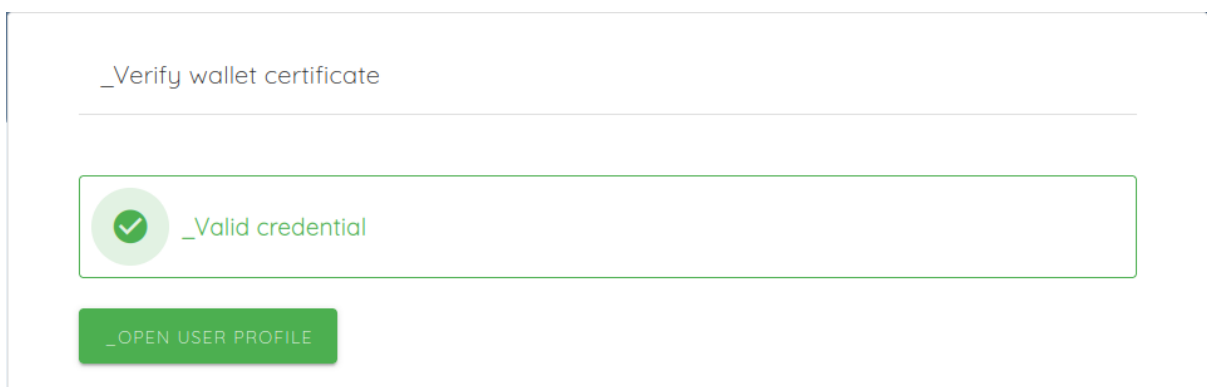
¹⁹ Verification portal



20

Once the connection request is accepted, the wallet of the user then shares the chosen VC (verifiable credential) in a format of a VP (verifiable presentation). The VP consists of one or more cryptographically signed VCs. It acts as a wrapper for verifiable credentials.

The third party can verify if the VP is valid or not. In this step, the third party already has access to the information of the verifiable credential and once confirming the validity, the data can be used for any purpose. A success message is displayed to inform that the verifiable presentation is valid.



21

²⁰ Request from the issuer to the user requesting a type of verifiable credential.

²¹ Verification process successful

Documental sources

ESCO (no date) *About Esco, ESCO*. Edited by European Commission. Available at:
<https://esco.ec.europa.eu/en/about-esco> (last accessed: 08 July 2023).

Europass Learning Model (no date) *Upcoming launch of the European Learning Model V3: Europass, Upcoming launch of the European Learning Model v3 | Europass*. Edited by European Commission. Available at:
<https://europa.eu/europass/tr/news/upcoming-launch-european-learning-model-v3> (last accessed: 08 July 2023).

European Commission (2020) 'Publishing of Qualification and Learning Opportunity Data Documentation'.

European Commission (no date a) *Conformant wallets, Conformant wallets - EBSI -*. Available at: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Conformant+wallets> (last accessed: 08 July 2023).

Pastor Matut, C. and Du Seuil, D. (no date) *Understanding the European self-sovereign identity framework (ESSIF), PPT*. Available at:
<https://www.slideshare.net/SSIMeetup/understanding-the-european-selfsovereign-identity-framework-essif> (last accessed: 08 July 2023).

Sporny , M., Longley , D. and Chadwick , D. (no date) *Verifiable credentials data model V1.1, W3C*. Available at: <https://www.w3.org/TR/vc-data-model/#abstract> (last accessed: 08 July 2023).

Sporny, M. et al. (no date) *Decentralized identifiers (DIDs) v1.0, W3C*. Available at:
<https://www.w3.org/TR/did-core/> (last accessed: 08 July 2023).

ValidatedId (no date) *Validated ID - electronic signature and digital identity providers, Validated ID - Electronic Signature and Digital Identity Providers*. Available at:
<https://www.validatedid.com/en> (last accessed: 08 July 2023).

Walt.id (no date) *Identity and NFT infrastructure for developers.*, *walt.id*. Available at:
<https://walt.id/> (last accessed: 08 July 2023).

Walt.id (no date) ,*Walt.id Web wallet*, *walt.id*. Available at:
<https://github.com/walt-id/waltid-web-wallet> (last accessed: 08 July 2023).