2025

D4.3 User Onboarding Guide

User Onboarding Guide For Credentials Issuing Online Platform

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

Document Change History

Version	Date	Author (organisation)	Description
V1.0	15 January 2024	Mikkel Egehave & Chris Mora-Jensen (Diplomasafe)	First draft
V2.0	26 March 2025	Mikkel Egehave & Chris Mora-Jensen (Diplomasafe)	Final draft

Table of Contents

List of Terms and Abbreviations

API	Application Programming Interface
CTDL	Credential Transparency Description Language
DID	Decentralised Identifier
DS	Diplomasafe
EBSI	European Blockchain Services Infrastructure
ECTS	European Credit Transfer and Accumulation System
ECVET	European Credit System for Vocational Education and Training
EDC	European Digital Credentials for Learning
EQF	European Qualifications Framework
ESCO	European Skills, Competences, Qualifications and Occupations
EU	European Union
EUDI	European Digital Identity
GDPR	General Data Protection Regulation
HR	Human Resources
JWT	JSON Web Tokens
MC	Micro-credential
REST	Representational State Transfer
URI	Uniform Resource Identifier
VC	Verifiable Credential
VET	Vocational education and training
VP	Verifiable Presentation
WCAG	Web Content Accessibility Guidelines
WP	Work Package

1. Introduction

The MCEU Hospitality project, a 36-month initiative funded by the European Union under the Erasmus+ programme, focuses on delivering five micro-credential courses that enhance digital and green skills for hospitality industry workers. Through this project, students receive verified credentials via an online platform fully interoperable with the European Blockchain Services Infrastructure (EBSI), the European Digital Credentials for Learning (EDC), and EUROPASS platforms.

The Credentials Issuing Online Platform developed in Work Package 4 allows VET Providers to issue, manage, revocate and share credentials as a result of learners successfully completing the five micro-credential courses. At the same time, learners can share, store and control access to their credentials. Finally, employers and business representatives will be able to validate the authenticity of micro-credentials presented.

Deliverable 4.3: The User Onboarding Guide is a crucial resource designed to facilitate the Installation and use of the Credentials Issuing Online Platform developed by Diplomasafe as part of Work Package 4. It provides a comprehensive, step-by-step guide for educational institutions and students, ensuring smooth navigation and use of the platform. It includes tutorials or screencasts, support ticket system, user feedback mechanism, and user support resources.

For educational institutions, the platform allows seamless issuance and management of credentials for students who complete the micro-credential courses. Institutions can customise diplomas in the project's official languages—Spanish, Danish, and Icelandic—ensuring alignment with their branding guidelines. The platform allows learners to receive, manage, and share their credentials with other educational institutions and potential employers, greatly enhancing their employability in the European hospitality sector.

This guide begins with an overview of the platform, covering initial setup steps for institutions and individuals, including account creation and login credentials. It comprises three main sections: installation to be done by the VET provider, one focused on functionalities available to students and another tailored for administrators at vocational education and training (VET) institutions. Additionally, the guide features standard sections on Support Services, Frequently Asked Questions (FAQs), and a Feedback System, ensuring users have access to assistance and can provide input on their experience.

The User Onboarding Guide (D4.3) is one of the useful resources to support VET providers in using the Diplomasafe's platform. This guide is designed to equip VET providers with the knowledge and skills needed to navigate and utilize the platform effectively. By following the step-by-step instructions and explanations provided, they will be able to issue and manage micro-credentials seamlessly.

The User Onboarding Guide (D4.3) is divided into the following sections:

- **Step-by-Step Instructions:** The guide includes clear and concise instructions that walk you through each process involved in using the platform.
- **Explanations and Clarifications:** Each step is accompanied by detailed explanations and clarifications to ensure a thorough understanding of the platform's functionalities.
- **Visual Aids:** Screenshots, diagrams, and other visual aids are incorporated to enhance comprehension and provide a visual representation of the platform's interface.
- **Troubleshooting Tips:** Common issues and challenges are addressed with troubleshooting tips and solutions to help you overcome any obstacles.
- **Best Practices:** Recommendations and best practices are highlighted to optimize your experience and

maximize the efficiency of your credential issuance and management.

2. MCEU Micro-credentials Pilot

The MCEU Consortium is piloting 5 micro-credentials on digital and green skills for the hospitality industry in two piloting rounds. Each institution - Idan, EUHT St Pol and UCN, will issue to all successful students a Verifiable Credential (VC) as proof of the completion of the courses (Task 5.4). Overall the MCEU consortium will deliver 500-micro-credentials. The issuing will happen at the end of the second and third years, after the courses roll-out.

A VC is a digital diploma or certificate, tamper-proof, highly secure, and offers numerous administrative advantages. VCs transform the way diplomas are issued and verified thanks to:

- **Security and Efficiency**: They combat credential fraud using cryptographic signatures, ensuring the authenticity of academic records.
- **Accessibility and Mobility:** They are easily stored in a digital wallet and can be shared internationally, facilitating student and labour mobility across the European Union.
- **Simplification of Administration**: They significantly reduce paperwork for universities and employers streamlining administrative processes.

The issued micro-credential will fulfil all the mandatory elements outlined in the EU Council Recommendation on micro-credentials (see Figure 1). Adjustments can be made by the Issuer to accommodate the exact needs of the issuance.

```
export type Credential = {
    id?: string;
    learnerName: string;
    learnerMail: string;
    title: string;
    issueDate: Date | string;
    country: string;
    criteria: string;
    credits: string;
    level: string;
    assessmentType: string;
    participationForm: string;
    verifiedBy: string;
    status?: Status;
};
```

2.1. Role of VET Providers and Administrators

VET providers (UCN, Idan and EUHT St Pol) will provide more than 500 learners the opportunity to follow 5 micro-credential courses on digital and green skills in the hospitality industry. After the successful completion of these courses, VET providers will issue a VC using the platform developed by Diplomasafe. In case of revocation, they will make all necessary changes and, when needed, they will revoke the VCs.

It is important to note that the VET providers in this project would need to obtain their own set of DID and keypairs certificates in order to issue to EBSI using this platform. The platform, once installed at hardware hosted at the VET, won't have the DID and Keypair identifying the VET as a TI. Diplomasafe has obtained the DID/keypair set for this project as a developer of the platform. Also the VET providers will need to go through the EBSI Conformity Test once the platform is installed and supplied with the TI DID and keypair.

3. MCEU Credentials Issuing Online Platform

The MCEU Credentials Issuing Online Platform is a comprehensive software solution designed by Diplomasafe to enable educational institutions, such as UCN, EUHT St Pol, and Idan, to issue VCs in a secure and efficient manner. This platform offers a robust backend interface that empowers educational institutions to meticulously review issued credentials and seamlessly provide new credentials to learners. Simultaneously, students can conveniently access and manage their credentials through a user-friendly wallet.

Embracing the principles of open-source software, the platform is publicly available on GitHub, fostering collaboration and transparency. Detailed instructions on how to install and configure the open-source platform are readily accessible on GitHub and are regularly updated to ensure compatibility and optimal performance.

As an open-source platform, it is essential to note that end-users, including VET and training institutions, are responsible for procuring suitable hardware and allocating necessary resources to install, update, maintain, and operate the platform effectively. To facilitate seamless integration with existing platforms used by VET and training institutions, the platform is equipped with comprehensive Swagger documentation.

Please note that the MCEU Credentials Issuing Online Platform is constantly evolving to meet the changing needs of educational institutions and learners. As new features are added and improvements are implemented, the platform may undergo updates and modifications.

To stay up-to-date with the latest information and ensure compatibility with the platform's current version, we strongly encourage you to refer to the project's GitHub repository. The repository contains the most recent documentation, resources, and announcements related to the platform.

4. Getting Started (installation)

Detailed and updated instructions for installation and operation of the platform can be found at https://github.com/Diplomasafe/mceu/tree/main.

The GitHub repository houses the complete source code necessary to deploy and operate the platform. The project has been containerized to simplify the installation process. However, please note that several prerequisites are essential for the platform's functionality. Where possible, these prerequisites have also been containerized, but they are not integral components of the platform itself. It is crucial to consider these prerequisites during the platform installation. **Please be aware that the following guide is provided as-is and may contain outdated information. For the most up-to-date documentation and instructions, always refer to the repository.**

4.1 Installation of prerequisites

If the target environment doesn't already have the following installed, then this is where we need to start:

- Docker
- Docker Compose
- Node.js (recommended)

We explain each element in detail below.

4.1.1 Docker and Docker Compose

Docker and Docker Compose is an essential part of installation, and will help the operator to have the platform running. It is installed by running a few commands in the terminal window of the server which will host the platform. The example is using a linux platform and the environment used by the VET may be different, and hence have an influence on the actual command execution. Before any installation is done, please remember to ensure the system is updated.

First we need the GPG key from Docker. This is done through a series of commands:

```
rpi@raspberrypi64:~ $ # Add Docker's official GPG key:
sudo apt-get update
sudo apt-get install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/debian/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc

# Add the repository to Apt sources:
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/debian \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
```

After updating the system and adding the GPG key we can move on to installing Docker and Docker Compose. This is also done through a simple command:

```
Reading package lists... Done
rpi@raspberrypi64:~ $ sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

This command will install Docker which we will use to get the actual platform up and running. for further information about docker please refer to the Docker main page and consult the documentation available.

4.1.2 Node.js

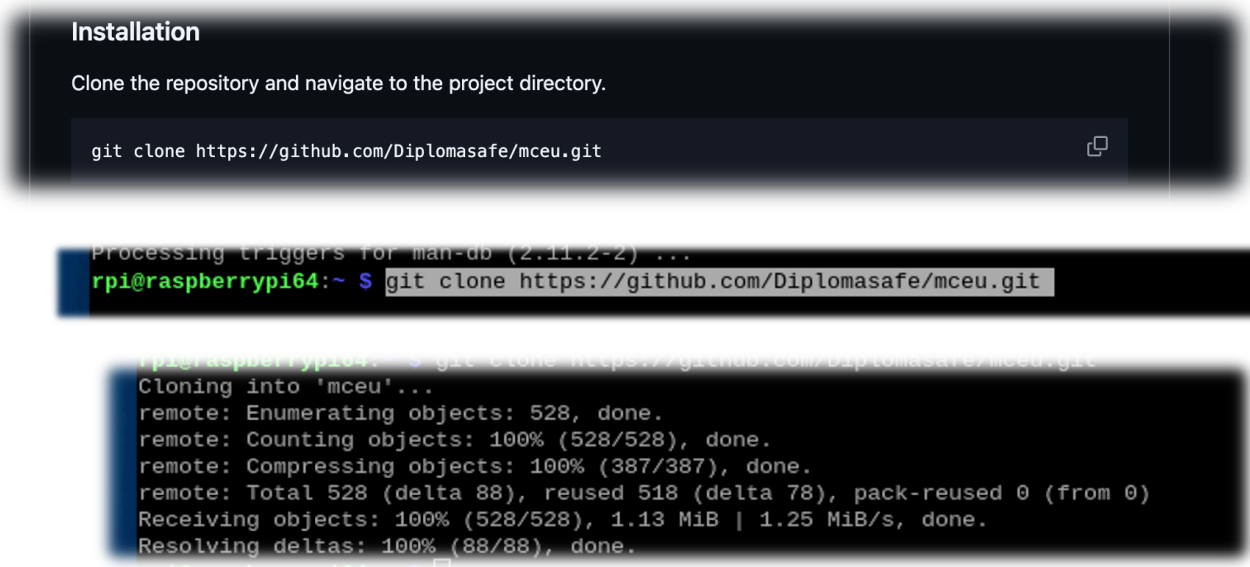
Even simpler than the docker installation, is the installation of node.js. Similar to Docker, a command is used to install the runtime environment.

```
rpi@raspberrypi64:~ $ sudo apt install nodejs npm
```

Once the node is installed, the platform environment is now prepped and ready for the installation of the actual platform.

4.2 Installation of the platform

The installation of the platform is done by cloning the software repository from GitHub. This can be achieved either through a GUI enabled git client, or simply by running the git clone command in a terminal window.



The command will essentially copy the complete repository to the local computer. Once cloned we can make the initial changes to start the platform. This is only a very basic setup, and more advanced scenarios can be created but will need additional changes which will not be covered by this guide. Also additional information can be available on the public github page for this project.

4.2.1 Adjusting the .env files

The cloned repo comes with the basic .env files, but they need to be renamed in order for them to actually work. Throughout the cloned repository you will find files all called ".env.example". These are usually hidden so we need to make sure they are shown by adjusting the OS view files settings. Once they are located, they need to have the ".example" removed making them just ".env", remember to save the files once the renaming has been done.

4.2.2. Starting the platform

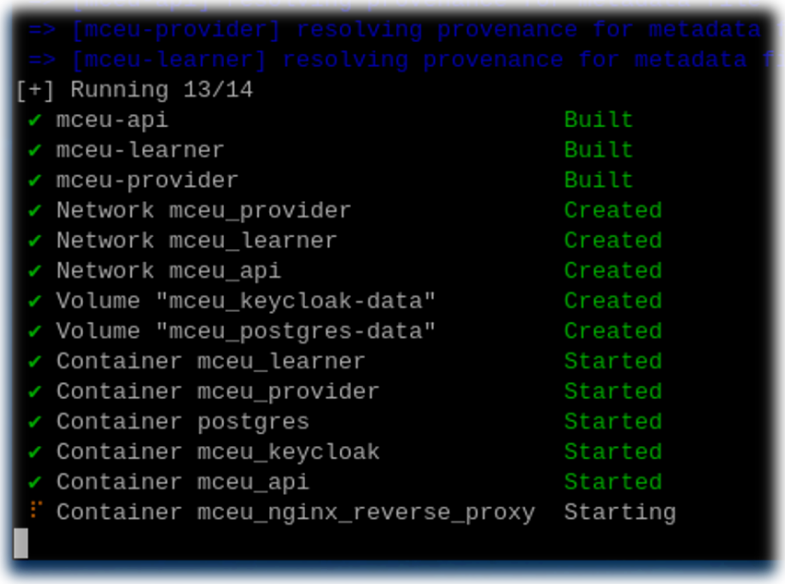
For a more complete guide and fully updated instructions along with additional tips for more advanced users please consult https://github.com/Diplomasafe/mceu.

To get the platform started once the prerequisites are in place, the repository has been cloned to the host environment and the necessary .env files are correct we can ask Docker to start all the containers. Depending on the hardware the platform is running on it can take some time.

To start the containers please run the following command.

```
rpi@raspberrypi64:~/mceu $ sudo docker compose -f docker-compose.yml \
              -f mceu-api/docker-compose.yml \
              -f mceu-learner/docker-compose.yml \
              -f mceu-provider/docker-compose.yml \
              up --build -d
```

This command will build and start the services included in the platform.



When all containers are up, the platform is essentially live.

Depending on the use, additional local changes to DNS, host files, firewalls etc may be required. The platform is provided with a basic skeleton which will allow the hosting entity to adjust and customize the look to their needs, or if preferred the provided GUI can be ignored and the platform can be integrated into an existing system by the use of the included REST API.

Currently the API is documented through swagger and can be found here, at the time of writing, https://stage-ds-api-wallet.diplomasafe.net/documentation#/, or for a more updated access, the swagger documentation is also available on the locally installed environment by simply navigating to the /documentation/ url of your installed platform.

4.2.3 About the hardware

The hardware requirements for this project are relatively low, as successfully demonstrated by its installation and operation on System-on-Chip (SoC) devices like the Raspberry Pi (tested on a Raspberry Pi Model 5 with 16GB RAM). However, it's important to note that running critical services on such a small device is not recommended due to potential performance and stability issues.

Significantly enhanced performance and stability can be achieved by running the platform on more powerful hardware. Given its relatively modest requirements, it's quite feasible to run the platform on existing hardware that supports Docker, as it can be deployed as a set of containers without encountering significant issues.

The following estimated specifications are sufficient for efficient system operation:

- **CPU:** 4 core CPU @ 2.5 GHz
- **RAM:** 8 GB
- **Disk Space:** 20 GB

Important Note: As the platform issues and manages more credentials, the size of the database will inevitably increase. This growth is a natural consequence of the platform's operation and should be anticipated. However, it's crucial to be aware that the platform possesses the flexibility to be reconfigured to leverage an existing database if necessary. This adaptability can be valuable in certain scenarios, such as when consolidating data or integrating with existing systems.

To safeguard against potential data loss due to unforeseen events such as hardware failures, software glitches, or human errors, it is imperative to establish and maintain a regular schedule of database backups. These backups should be performed frequently and stored securely in a separate location to ensure that, in the event of data loss, the information can be recovered swiftly and with minimal disruption to the platform's operation.

Additional Considerations for Hardware Selection:

- **Storage Type:** While the disk space requirement is 20GB, consider using faster storage options like Solid State Drives (SSDs) for improved system responsiveness, especially database operations.
- **Network Connectivity:** Ensure reliable and sufficient network bandwidth for smooth operation, especially if the system will be accessed by multiple users or handle large amounts of data.
- **Scalability:** If future expansion or increased workload is anticipated, select hardware that allows for easy upgrades or scaling of resources, such as additional CPU cores, RAM, or storage.
- **Redundancy and Fault Tolerance:** For critical deployments, consider hardware redundancy options like RAID (Redundant Array of Independent Disks) for storage or failover mechanisms for network connectivity to minimize downtime in case of hardware failures.
- **Power Supply:** Ensure a stable and reliable power supply for the hardware to prevent unexpected shutdowns or data corruption.
- **Cooling:** Adequate cooling is essential to prevent hardware overheating and maintain optimal performance.
- **Hardware Compatibility:** Verify compatibility of the chosen hardware with the operating system and Docker environment to avoid potential conflicts or issues.

5. VET Providers Interface

VET Providers access and use the platform to perform different actions:

- Manage user accounts for instructors and learners, assigning specific roles. They securely register learners on the platform.
- Issue verifiable micro-credentials to learners that have successfully completed the courses.
- Revocate credentials in case of expiry, fraudulent representation and misuse of certification.
- Share efficiently and securely the credentials with external institutions and employers, with the learner's approval.

5.1. Dashboard Overview

The MCEU Credentials Issuing Online platform features a lightweight dashboard design. This is primarily due to its open-source nature, which allows for individual customization by the end-user (VET and training institutions).

This approach ensures that the platform remains nimble and adaptable, avoiding unnecessary bloat and allowing each institution to tailor the dashboard to their specific needs. Instead of a fixed, feature-heavy interface, the platform provides a core foundation upon which institutions can build.

This customizability extends to:

- **Appearance:** Institutions can modify the visual elements of the dashboard to align with their branding and aesthetic preferences.
- **Functionality:** Specific features can be prioritized or added, depending on the institution's workflow and requirements.
- **Integration:** The platform can be integrated with existing systems through the provided REST API, further enhancing its flexibility and reducing the need for a complex, all-encompassing dashboard.

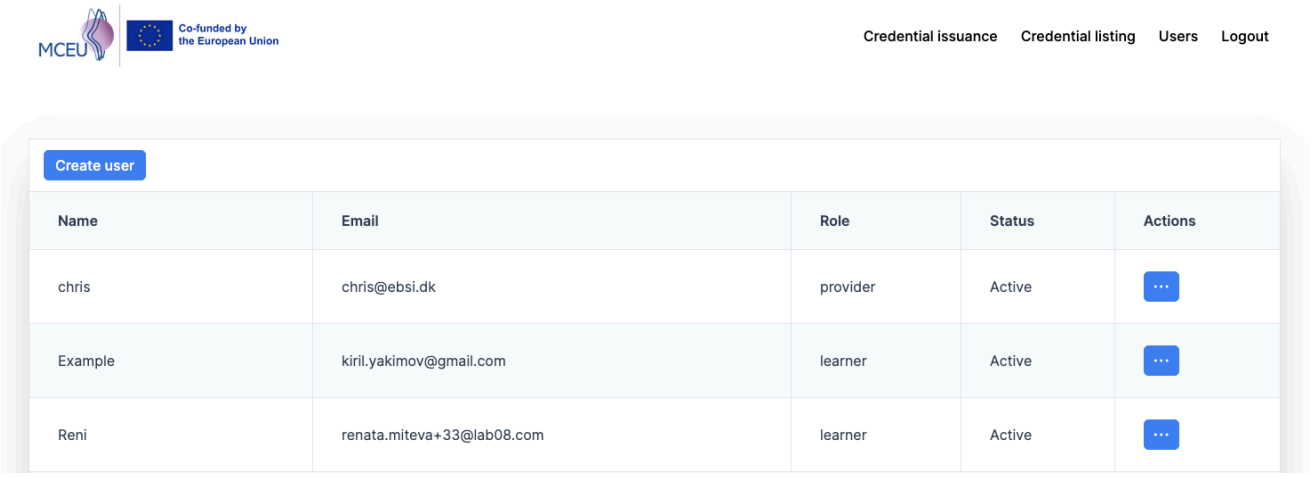
By keeping the core dashboard lightweight, the platform ensures optimal performance and responsiveness, even on less powerful hardware. This also simplifies maintenance and updates, as institutions only need to manage the customizations they have added, rather than navigating a complex, monolithic system.

5.1.1. Navigation Bar

A navigation bar in the top of the page provides a few options for the VET provider. Aside from the Logout item, which naturally logs the user out, three other options exist:

- **Users Menu**: interface for creating and deleting users. Covers both receivers and platform administrators.
- **Credential Listing**: overview and status of issued credentials.
- **Credential Issuance**: issuance interface for platform administrators.

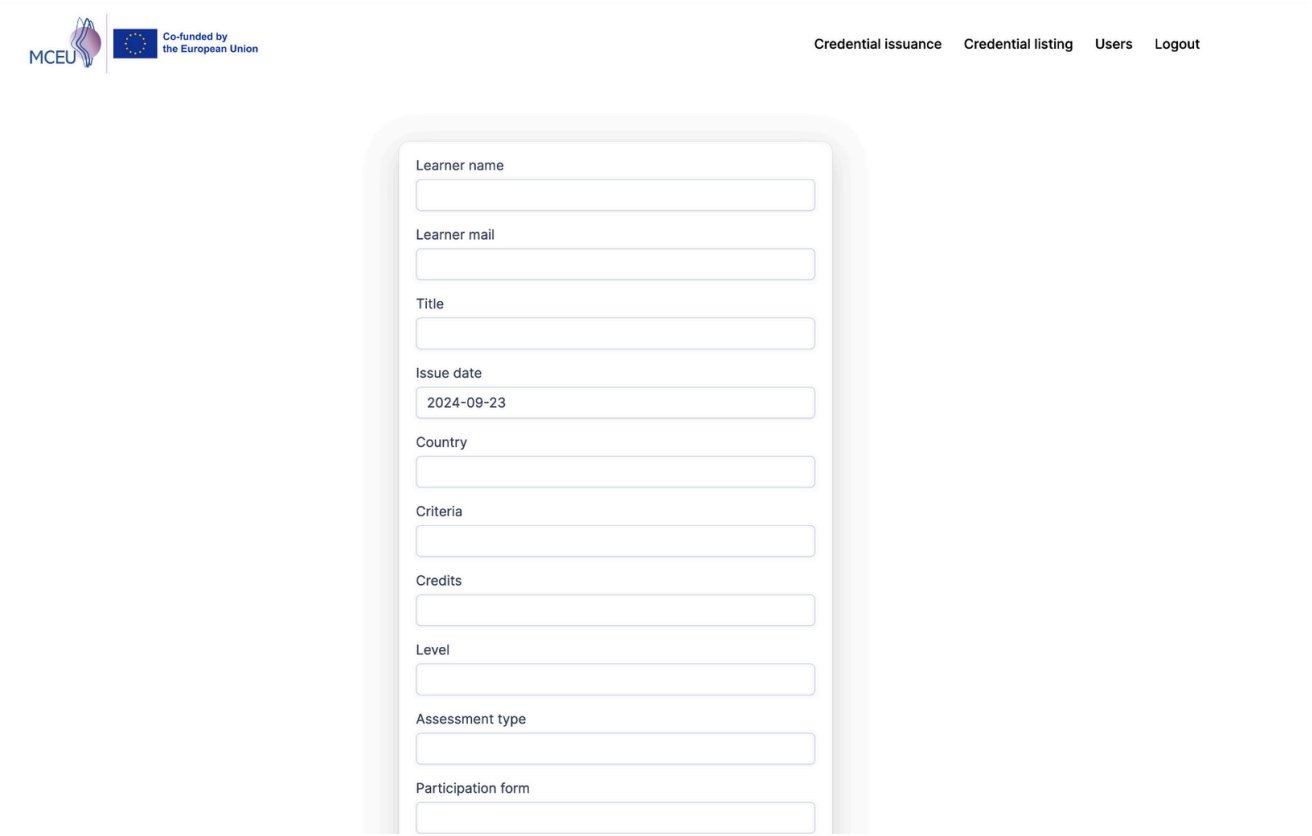
5.2. User Management



Page button for opening a create from modal and with a table that shows user information fetched from the RestAPI. Every table row will have action buttons for updating and deleting users. Here, they can:

- **Create (C)**: Add new users to the system by filling in necessary details like name, username/email, password, and role (Admin or VET Provider).
- **Read (R)**: View the list of all users in the system, along with their details.
- **Update (U)**: Edit the details of existing users, such as their role, status, or email.
- **Delete (D):** Remove users from the system if needed.

5.3. Credential Issuance

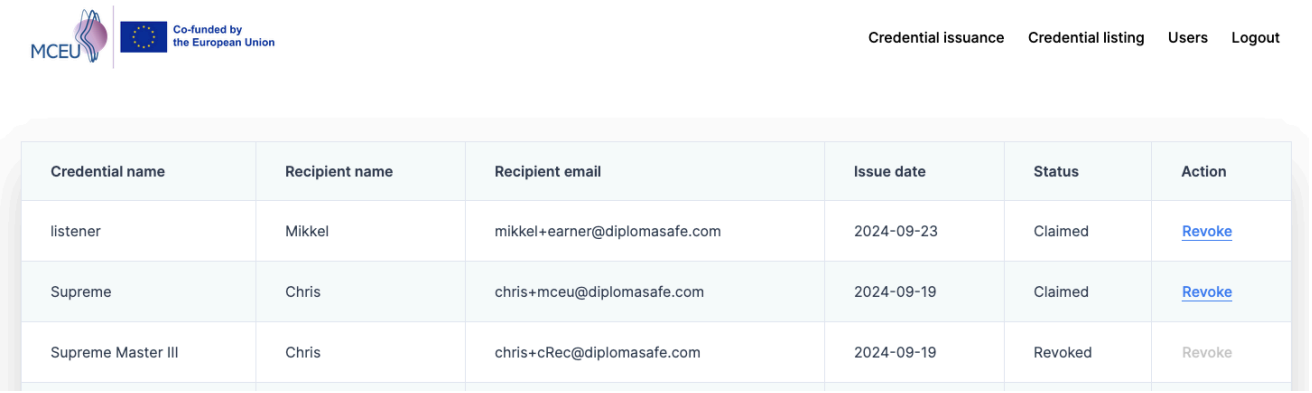


Form page from issuing credentials based on the previously created templates. They can:

- Select a template from a dropdown list containing all available templates.
- Fill in the required information (such as learner details, completion date, etc.) to issue a diploma either from a file or based on filled fields (depending on the selected radio button).

Once all necessary details have been filled in, they can proceed to issue the credential.

5.4. Credentials Listing



This Diploma Management feature will let VET Providers have granular control over the credentials they issue and manage. This page will provide the option to manage previously issued diplomas. VET Providers can choose two functions: Read and Revoke.

5.4.1. Read

This function allows the VET provider to view the details of all issued credentials in a table format. This could include details like the learner's name, course completed, date of issuance, and status of the diploma/credential (claimed/unclaimed).

Credential Management Dashboard

This dashboard provides a comprehensive overview of all issued credentials in a user-friendly table format. Each row represents an individual credential and displays the following details:

- **Learner Name:** The full name of the recipient of the credential.
- **Course Completed:** The specific course or program for which the credential was awarded.
- **Date of Issuance:** The exact date when the credential was issued.
- **Credential Status:** Indicates whether the credential has been claimed or remains unclaimed by the recipient.

The table can be sorted and filtered by any of the displayed columns to facilitate easy searching and organization. Users can also export the table data in various formats for further analysis or record-keeping.

5.4.2. Revoke

This functionality provides VET Providers with the ability to revoke or invalidate a credential that has been previously issued. This action would result in a change in the credential's status from "active" to "revoked," indicating that it is no longer valid or recognized.

Reasons for revoking a credential might include:

- **Academic dishonesty:** If a student is found to have cheated or plagiarized their work, the credential may be revoked.
- **Professional misconduct:** If a credential holder engages in behavior that violates professional standards or ethics, the credential may be revoked.
- **Administrative error:** If a credential was issued in error (e.g., to the wrong person or with incorrect information), it may be revoked.
- **Completion of additional requirements:** In some cases, a credential may be revoked if the holder fails to complete additional requirements (e.g., continuing education credits).

The process for revoking a credential may vary depending on the VET Provider and the specific circumstances. However, it typically involves notifying the credential holder of the revocation and updating the credential's status in the relevant database or registry.

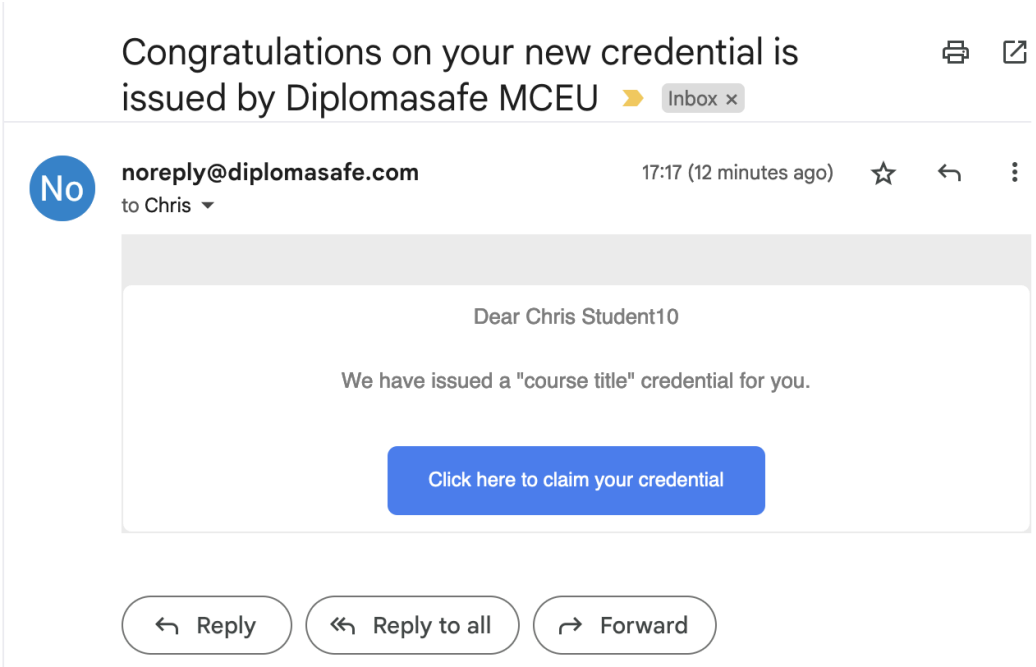
6. Student Interface

6.1 Communication

When a credential is issued from the platform, the recipient will receive an email notification at the address provided during the credential submission process. This email will inform them that a credential is waiting to be claimed.

The platform includes a basic email service to facilitate this notification process. However, this service can be replaced with any preferred external email service that the VET provider may already have in place.

It's important to note that opting for an external email service will necessitate a number of configurations and adjustments on the VET provider's end. These changes will ensure seamless integration between the platform's credential issuance process and the chosen email service, guaranteeing that recipients are promptly notified of their awaiting credentials.



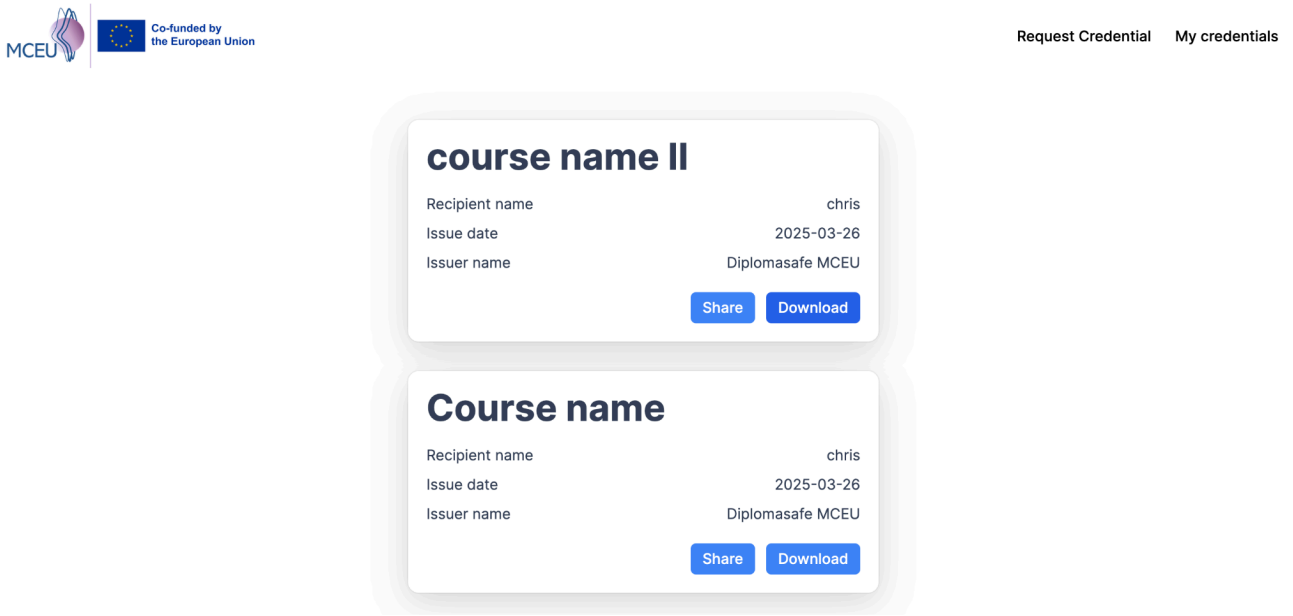
While the platform's default email service offers a reliable and efficient way to deliver diploma claims, institutions may opt to replace it with a communication method better suited to their local context. For instance, organizations operating within Denmark could integrate with the national communication service "e-Boks," streamlining the delivery process and aligning with established practices.

Once the diploma claim has been sent via the chosen communication channel, the recipient can simply click on the provided link to initiate the claiming process. This action seamlessly redirects the learner to the recipient's platform, where they can securely access and manage their digital diploma. This integration

ensures a smooth and user-friendly experience, allowing learners to effortlessly transition from the notification to the actual diploma claim.

6.2 Receivers view/3rd party view

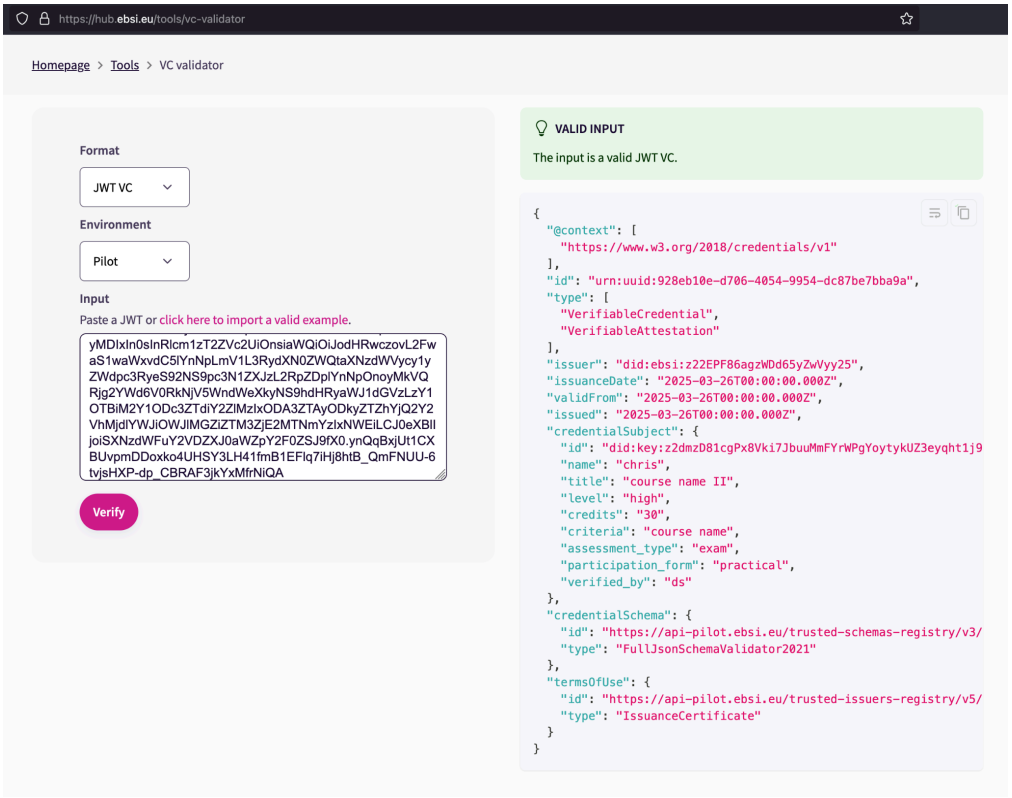
Upon initiating the claiming process, the recipient will find the credential issued and displayed within their platform view. The next time the recipient accesses the platform, they will be prompted to replace the provided temporary password. After changing the password, the recipient will gain full access to their account. This account will serve as a repository for all the credentials the recipient has earned and been awarded by the VET provider.



When recipients receive a credential, they have the option to generate a shareable link for that credential and copy it to their clipboard. This link can then be shared with others. It's important to note that the shareable link directs to a 3rd party view of the platform. This means that the link will only function as long as the VET provider continues to operate the platform. Additionally, the appearance of the link will follow a specific format, similar to this example:

https://stage-ds-learner-wallet.diplomasafe.net/credentials/928eb10e-d706-4054-9954-dc87be7bba9a

Furthermore, the recipient has the option to download the JWT token. This token can be utilized for manual credential verification, if necessary. To do this, the recipient can navigate to the following website: https://hub.ebsi.eu/tools/vc-validator. On this page, they can paste the JWT into the provided field and click the "Verify" button. This process allows for an additional layer of security and ensures the authenticity of the credential.



If the provided JSON Web Token (JWT) is invalid, the VC validator tool will gracefully handle the error and inform you that the provided token cannot be validated. This may be due to a variety of reasons, such as an expired token, an incorrect signature, or a mismatch between the expected and provided claims.

7. Modifications

The platform's frontend and backend code is designed to be adaptable and customizable to meet evolving user requirements. The codebase is open-source and hosted on GitHub, providing developers with the ability to fork the repository and implement modifications. This open development model fosters a collaborative environment where contributions from developers of all skill levels are encouraged and welcomed.

By making the code open-source, the platform promotes transparency and facilitates innovation. This approach ensures that the platform remains agile and responsive to the changing needs of its users. Furthermore, it establishes a community-driven development model, where users can actively participate in shaping the platform's future and direction.

The availability of the code on GitHub allows developers to easily access and review the code, identify areas for improvement, and propose changes. The development community actively supports collaboration and provides guidance to developers who are interested in contributing. This collaborative approach not only accelerates the development process but also ensures that the platform benefits from a diverse range of perspectives and expertise.

Overall, the open-source nature of the platform's codebase is a key factor in its ability to adapt and grow. It fosters a sense of ownership and empowerment among users, while also ensuring that the platform remains at the forefront of technological advancements.

8. Conformity testing

After the successful installation of the MCEU Credentials Issuing Online Platform on the local servers of a VET provider, the subsequent and critical step is to conduct the EBSI Conformity Test. This test holds immense importance due to the fact that the platform, in its initial setup, is not equipped with the necessary DID and keypair. These are essential elements that uniquely identify the VET provider as a TI within the expansive framework of the EBSI.

Diplomasafe, the entity responsible for developing the platform, does possess an initial DID/keypair set that was used during the development phase. However, it's of paramount importance that each VET provider establishes its own distinct and unique identity within the EBSI ecosystem. The successful completion of the Conformity Test serves as a confirmation that the VET provider's platform adheres to the required configuration and possesses the necessary authorization to issue verifiable credentials. These credentials, in turn, are recognized and validated throughout the EBSI network.

This validation process is vital as it preserves the integrity and interoperability of the issued micro-credentials, ensuring that they are trustworthy and can be seamlessly utilized across different systems and institutions within the EBSI network.

9. Conclusion

The MCEU Credentials Issuing Online Platform has the potential to revolutionize the issuance and management of micro-credentials. By streamlining processes, enhancing efficiency, and promoting transparency, the platform will benefit both educational institutions and learners.

Thank you for choosing the MCEU Credentials Issuing Online Platform and for being a part of the MCEU project. We value your participation and are committed to providing you with the support you need to succeed. If you have any questions or encounter any difficulties while using the platform, please do not hesitate to reach out to our support team.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them