2024

Credential Issuing Online Platform - Requirements Document

D4.1 REQUIREMENTS DOCUMENT

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	21 Feb 2024	Mikkel Egehave & Chris Mora-Jensen (Diplomasafe)	First draft
V2.0	27 Feb 2024	Sigurður Fjalar Jónsson (IDAN) Anne Mette Uttrup Brügge (UCN) Erica Martinelli (Access Advisors)	Partners' feedback
V3.0	29 Feb 2024	Mikkel Egehave & Chris Mora-Jensen (Diplomasafe)	Final draft

Contents

1. List of Terms and Abbreviations

API	Application Programming Interface
CTDL	Credential Transparency Description Language
DID	Decentralised Identifier
DS	Diplomasafe
EBSI	European Blockchain Services Infrastructure
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
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

2. List of Tables

3. List of Figures

1. Introduction

The MCEU Hospitality project, funded under the Erasmus+ initiative, is dedicated to advancing digital and green skills within the hospitality sector across Denmark, Iceland, and Spain. As part of Work Package 4 (WP4), learners will receive verified credentials through a Credentials Issuing Online Platform (hereinafter: the platform) designed by Diplomasafe. This portable digital micro-credential platform will offer a user-friendly, reliable, interoperable, and compliant solution for creating, storing, sharing, and verifying certificates.

Diplomasafe will guarantee that the platform is in alignment with the latest European Union (EU) regulations and integrated with existing EU tools and infrastructures, including the European Digital Credentials for Learning (EDC), European Blockchain Services Infrastructure (EBSI), and Europass. Moreover, the infrastructure supporting data storage will be based on open standards and data models, facilitating interoperability and secure data exchange to ensure authenticity.

The platform will comply with the Council of the European Union's (EU) "Recommendation on European approach to micro-credentials for lifelong learning and employability," adopted on 16 June 2022. This document sets a defined structure for micro-credentials, principles for their design and issuance, and quality assurance mechanisms.

Hence, the platform will adhere to the ten principles outlined in the Recommendation, encompassing aspects such as Quality, Transparency, Relevance, Valid Assessment, Learning Pathways, Recognition, Portability, Learner-Centred design, Authenticity, and provision of Information and guidance (see Annex A). These standards ensure quality, transparency, cross-border compatibility, recognition, and micro-credential portability (Council of the European Union, 2022).

Diplomasafe will define the platform's requirements to ensure it addresses end-users' needs and specificities within the hospitality sector (Task 4.1). This entails collecting the needs of end-users, primarily VET providers in Denmark, Iceland, and Spain, who will utilise the online platform to issue micro-credentials to learners. The analysis is complemented by a stakeholder mapping, formulated in Task 2.1, user needs analysis, user scenarios and journeys to describe the platform functioning.

The **Requirements Document** (Deliverable 4.1) outlines essential features and functionalities necessary for the design and development of the platform to meet the needs and expectations of users and stakeholders. The analysis begins with an overview of the key target groups, including learners, VET providers and relevant stakeholders It presents three user scenarios and journeys before delineating required functionalities for the platform and interoperability considerations.

2. Users' Needs Analysis

The platform must respond to the needs and expectations of a variety of stakeholders, namely VET Providers, Learners, Employers including Business Representatives. These stakeholders will access and use the platform to perform different actions as part of the issuance, verification and validation of micro-credentials. Table 1 outlines the characteristics of each user group and their roles in the online platform.

Table 1: Platform user groups, their needs and roles

User Group	Needs	Roles
VET Providers	**Streamlined workflows** for issuing micro-credentials, ensuring secure, verifiable, and cost-effective ways to issue, manage, and revoke credentials. **Comprehensive support services** to effectively utilise the platform, including training and technical assistance tailored to their needs. **Robust data security measures** to protect learner information and ensure the integrity and confidentiality of issued micro-credentials based on international education standards and data privacy laws (e.g. General Data Protection Regulation). **Seamless integration** with existing student information systems within the institution and with other institutions and industry credentials. **Customizability** to align with each VET provider' branding and language. **Scalability** to accommodate a growing number of digital credentials and **stackability** to allow professionals to accumulate micro-credentials over time. **Reporting features** to track the usage and status of issued certifications.	**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.

Learners	**Accessible platform interface** that facilitates easy navigation and accommodates learners of varying backgrounds and digital literacy levels. Preference for mobile access for ease of sharing and verification. **Seamless management** of earned micro-credentials, including the ability to access, share, store and verify credentials securely across borders to enhance employability and mobility within the Hospitality industry. **Be informed** about their credential status. **Assurance that credentials** will be recognised by educators and employers across borders. **Control over who gets access to their data**.	**Request the issuance** of a micro-credential to certify the acquired skills. **Share credentials** with potential employers and other users via digital or print credential. **Store the micro-credential** in a lifelong secure holder wallet (e.g. Europass, EBSI), in line with the General Data Protection Regulation. **Control access** to their credentials and educational data.
Employers and Business representatives	**Reliable verification process** to validate the authenticity and relevance of micro-credentials presented by job candidates. **Rapid and real-time verification process** that enables quick and accurate validation of micro-credentials during the recruitment process. **Access a diverse pool of skilled candidates** with verified micro-credentials in green and digital skills, facilitating recruitment and talent acquisition efforts aligned with industry priorities. Integration with professional platforms and internal Human Resources (HR) systems.	**Validate the authenticity** of micro-credentials presented by potential hires, including the identity of the credential-holder (learner), the legal identity of the issuer (VET Provider), date and place of issuance.

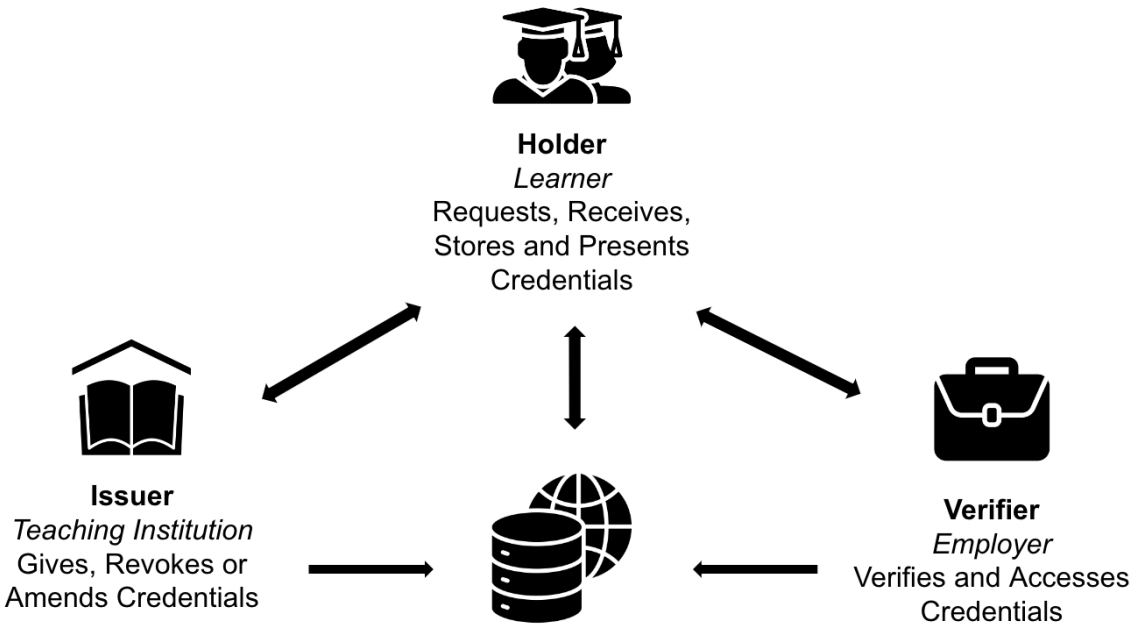
Based on the analysis of the Users' needs and roles, the development of the Credentials Issuing Online Platform will adopt the following principles:

- **Customization and Integration:** The platform is adaptable to the specific systems and processes of each user group in the Hospitality sector. This includes the integration with existing institutional platforms.
- **User-Centric Design**: Ensure that the system is intuitive for learners while also being robust enough for the more complex needs of institutions and organisations.
- **Education and Support:** Provide assistance, technical support and resources including FAQs to VET Providers, Learners and Employers to use the platform.
- **Data Privacy and Security**: The platform will adopt a strong focus on data security, ensuring that all user data is protected and that users retain control over their information, in line with relevant regulations, such as the General Data Protection Regulation (GDPR).
- **Global Standards Compliance**: Ensure the platform adheres to international credentialing standards to facilitate widespread acceptance and portability.
- **Cross-Sector Collaboration**: Foster partnerships with both VET Providers and corporate entities to ensure the platform is well-tailored to the Hospitality Sector market's needs.

3. User Scenarios & Journeys

The Credentials Issuing Online Platform allows VET Providers, Learners and Employers/ Business Representatives to obtain, validate, store and exchange micro-credentials as shown in Figure 1.

Figure 1: Credential lifecycle



To build a user-friendly platform, we identified different scenarios and journeys to describe the issuance, verification and revocation of the Verifiable Credentials.

3.1. Micro-Credential Issuing (VET Providers)

The objective of this process is to issue the micro-credential upon the successful completion of the digital and green skills courses provided on Lobster Ink's platform.

1. Learner Registration

Learners log into the Credentials Issuing Online Platform (integrated with the VET provider's portal/ course provider's portal).

→ Case 1: User is already registered on the Platform

- Learner authenticates using their pre-existing DID and Proof of Identity, proving their identity on the system without the need to enter personal details.
- The platform verifies provided student data securely, based on the DID/signature.

2. Credential Preparation

Once the learner successfully completes the course, the VET Provider (issuer) issues a Verifiable Credential, as follows:

- The issuer gathers all required information for the micro-credential, ensuring that it complies with the features established in the Council of the EU's Recommendation (see Annex A). The same format and attributes are defined in the schema already registered in the Platform, ensuring that the VC is universally recognizable and verifiable by any party.
- As the VC is prepared, a reference to the schema (an identifier or a URI) is embedded within the credential itself. This tells any verifier which schema the VC adheres to.
- The issuer signs the VC using its private key associated with its DID. The resulting signature is embedded within the VC.

3. Credential Issuance

→ Case 1: VC is automatically issued to the user on course completion

- Learners are notified about the availability of the credential (by available means such as mail, mobile notification, SMS, etc.).
- Learner authenticates into the platform and accesses the credential for approval.
- Pathway 1.1: User requests data modification due to errors/mistakes. In this case internal review from the VET Provider will be activated.
- Pathway 1.2: User verifies credential data and approves its delivery to the wallet (if available)

3.2. Micro-Credential Request and Verification (Employers)

This process enables employers and institutions to verify the authenticity of the Micro-credential.

1. Employer Requests Certification

A verifier organisation (e.g. employer or another institution) requests a credential to a user specifying the means of receiving this credential. In case of a user with a holder wallet, the wallet requests consent from the user to share the credential. Otherwise the request can happen in different ways, for example:

- A web portal where the user logs in and gets prompted to share their VC (EUDI -enabled student receives a verification request notification).
- An enterprise wallet (EUDI-enabled student receives a verification request notification).
- A QR code mechanism where the user scans the code with his/her holder wallet to initiate the VC sharing.

→ Case 1: The requesting enterprise is NOT an Authorised verifier. The holder wallet notifies the user that this organisation isn't pre-authorized and provides comprehensive details about which specific data the requester

seeks. The holder wallet seeks the user's consent to share the VC using a Selective Disclosure feature, which restricts the amount of data that will be disclosed.

→ Case 2: The requesting organisation is an Authorised verifier. Holder wallet informs the user that the organisation is a pre-authorized entity and requests permission to share VC.

- After reviewing the request, the student gives consent (ensuring General Data Protection Regulation compliance) and issues a Verifiable Presentation (VP) containing the set of data as specified by the request and sign the request with his/her private key linked to personal DID
    - Note: user may own more DIDs connected to his identity.
- Holder wallet asks user confirmation if he/she wants to limit the verification process to a specific timeframe or a specific number of verifications.
- Holder wallet shares VP with the requesting institution (using alternative sharing means as specified in the request).
- Upon successful completion, the EUID informs the user that the Verifiable Presentation (VP) has been delivered successfully.

2. Credential is verified

- Verifier's enterprise wallet receives VP shared by the user
- Verifier's enterprise wallet verifies the holder's signature on the VP using the holder's DID Document from the EBSI ledger (which contains the public key).

→ Case 1: If constraints set by the user are matched (e.g., time frame allowed for verification or number of verifications), Verifier's enterprise wallet unpacks the VP to access the embedded VC(s) and verify the original issuer's signature on the VC(s). This is done using the issuer's public key, which can also be retrieved from their DID Document on the EBSI Trust Registry.

- Once verification is complete, the verifier will provide feedback or an acknowledgment to the holder, depending on the context (e.g., granting access to a service or confirming the authenticity of the shared data).
- A verification report is generated and stored on EBSI for transparency and traceability and the user gets notified accordingly.

→ Case 2: If constraints set by the user are NOT matched, the user gets notification that the verification tentative failed due to constraints. VC cannot be verified.

3.3. Micro-Credential Revocation (VET Providers)

The VET provider can decide at any moment to revoke the issuance of a micro-credential in cases of fraud or under exceptional circumstances. As a result, the credential is no longer valid. The conditions, authority and timing for the revocation of credentials can vary depending on the national legislation.

The wallet is built in a way that certifications include revocation rules, therefore revocation is performed at wallet level, with approval of the user or without depending on the applicable legislation. In this way the user will not be able to share anymore his certificate and any further verification will fail.

3.4. Possible Journeys and Scenarios

Based on the three processes described beforehand, we describe potential user journeys, namely the Issuance of the MCEU Micro-credentials and the Revocation and Re-Issuance of a Micro-credential.

Journey 1: Micro-credentials Issuance

Scenario: Rafael, Spanish student who completed the MCEU micro-credential course on green and digital skills in the Hospitality sector, applies for a job in a Hotel in Barcelona.

Step 1: VET Provider's academic board verifies that the student has completed the micro-credential course and is eligible for a certificate.

Step 2: VET Provider gathers the information and creates a Verifiable Credential, which includes the mandatory elements established in the Council of the EU's Recommendation and the institution's digital signature.

Step 3: The Credential is signed using the VET Provider's private keys to ensure authenticity and integrity.

Step 4: VET Provider informs Rafael that the VC is available and provides the needed instructions to retrieve it through the platform.

Step 5: Rafael accessed the platform to retrieve the Credential.

Step 6: Rafael shares his Credential directly with the potential employer or on social networks via a shareable link.

Step 7: Hotel in Barcelona verifies the credential by verifying the digital diploma by checking its

cryptographic proofs against the public keys recorded in the platform.

Journey 2: Micro-credential revocation

Scenario: Kristjan is an Icelandic student who enrolled and completed the MCEU Hospitality courses provided by Lobster Ink. He received a VC but noticed his surname was misspelt, requesting the Issuer to amend it.

Step 1: Kristjan records this request through issuance of a replacement request VC in EBSI. Kristjan reports the issue through the institution's enterprise wallet portal or contacts the administration sharing the created VC with the institution's wallet.

Step 2: The institution receives in its enterprise wallet the replacement VC, verifies the reason for replacement and confirms the need of replacing the existing Diploma.

Step 3: Institution use its enterprise wallet and calls EBSI-VECTOR revocation service to revoke diploma, e.g., the DID Document is updated to indicate the credential is revoked and creates a new digital diploma in the form of a Verifiable Credential, which includes corrected metadata and claims about the student's achievements and the institution's digital signature.

Step 4: The VET Provider notifies the student that his diploma card has been replaced

Step 5: Kristjan accesses his wallet, which could be a secure app or online service, to retrieve the digital diploma VC.

Journey 3: Employer verification

Learners can get fast and convenient access to their records and share it securely with potential employers. It also eases the burden on employers as they don't have to go through the background verification processes to confirm the student/applicant's accomplishments.

Scenario: Ella who successfully obtained the VC for the MCEU micro-credential course applies for a job in Denmark.

Step 1: The Danish employer requests proof of Ella's micro-credential.

Step 2: Ella shares her VC from the MCEU course via her wallet using standard means (e.g., email).

Step 3: The Danish employer logs into the platform and verifies the micro-credential authenticity and proceeds with the hiring process

4. Requirements and Functionalities

Based on the Users' needs, the platform will comply with a variety of technical and semantic requirements and functionalities, as Table 2 outlines. The list works as a reference and guide for the platform design and development.

Table 2: List of requirements and functionalities of the Credentials Issuing Online Platform

Category	Requirements	Functionalities
Technical requirements	**User onboarding & Profile management**	• User identification based on eIDAS regulation (L3) • Secure authentication with minimum eIDAS L3 level of assurance. • User self-sovereign profile creation with multiple contact channels (email, notifications, phone, social, etc). • User-friendly user interface both mobile and web based. • Multiple digital identities capability • OneTime Identity creation capability • Pin protection
	Credential issuance	• Ability for VET Providers to issue digital micro-credentials. • Customisable credential templates • Full portability of credentials with different e-wallets. • Capability to issue credentials in bulk. • Multi-signature and multi-issuer credential management
	Credential management	• Ability to list issued credentials. • Ability to view in detail an issued credential • Capability to export digital credentials in PDF format to be printed.
	Credential Access	• Capability to request, store and share digital credentials • Selective Disclosure, e.g., capability to share a subset of data present in the credential without disclosing all data • Ability for users to choose who can access their credentials and how long they can be accessed for, including one-time access sharing for one-shot verification. • Multiple sharing methods including full machine2machine methods • Shareable credential links for ease of access for employers or institutions and request credentials from users to be shared directly with the enterprise wallet.
	Credential verification	• Machine-based real-time Verification: ○ Employers and VET providers can automatically

		verify received credentials in real time without human intervention. ◦ Monitored access to blockchain-based credential anonymized references for authenticity verification. • Verification Reports: ◦ Generate GDPR-compliant verification reports and verification history. ◦ Timestamped verification records for audit trails. • Verification Revocation: capability for users to stop/deny verification from selected parties.
	Holder Wallet	• Secure wallet for users to manage their credentials.
	Privacy Data Control	• Compliance with data protection regulations (e.g. GDPR). • Auditable user consent management for data sharing. • Permanent data export and deletion options.
	Interoperability	• Open-source format • Compatibility with other digital systems and EU Platforms (e.g. EBSI, Europass, EDC) • Application Programming Interfaces (APIs) for integration with VET Providers' systems and employers' HR platforms.
	Standards Compliance	• Compliant with the European standard elements to describe a micro-credential
	Notifications	• Credential Updates notifications • Credential issuing process status notifications. • Expiry alerts for time-sensitive credentials. • Warning alerts for unsuccessful access to verification process
	User feedback and ratings	• Feedback mechanism for users to rate and provide feedback on credential issuers.
	Compliance and security	• Regular security audits and updates to ensure data protection. • Compliance with relevant educational and privacy regulations. • Compliance with cybersecurity directives (e.g. NIS).
	Stackability	• Stackable option to create more comprehensive certifications starting from multiple micro-credentials.

	Support and Help Center	• Help Centre with FAQs, tutorials, multi-language user support options.
Semantic requirements	**Standardised Credential Structure**	• The format of the credential will follow the mandatory requirements set in the Council of the EU's Recommendation (see Annex A).
	Language	• In addition to English, support partner VET Providers' national languages (Danish, Spanish and Icelandic) for credential data, mobile and web front end, data formats.
	Accessibility	• Web Content Accessibility Guidelines (WCAG), to provide a user-friendly experience for users with disabilities, ensuring inclusive access to digital credentials.
	Linked Data	• Implement Linked Data principles to enable the creation of globally unique and resolvable Uniform Resource Identifiers (URIs) through DIDs for VET providers, courses, and individuals. This supports the creation of verifiable credentials with contextual links.
	Educational Ontologies	• Use established educational ontologies, such as Schema.org Education Extension or the Credential Transparency Description Language (CTDL), to define vocabulary and terms specific to educational data. This ensures semantic consistency and alignment with existing educational standards.
	Credential Verification	• Incorporate mechanisms for credential verification and validation, enabling third parties to verify the authenticity and integrity of a verifiable credential by checking against the issuer's public key and relying on DIDs for verification.
	Contextual Information	• Include contextual information in verifiable credentials, such as course descriptions, competencies achieved, and relevant metadata, to provide a comprehensive understanding of the credential's significance.
	Consent and Privacy	• Implement consent management mechanisms that allow individuals to control the sharing of their verifiable credentials, ensuring compliance with data privacy regulations like GDPR. Provide transparency on how data is used and shared.
	Revocation and Expiry	• Specify semantic requirements for handling credential revocation and expiry, enabling authorised entities to revoke or update credentials as necessary while maintaining the integrity of historical data.

	Interoperability Standards	• Align with interoperability standards, such as JSON-LD and JSON Web Tokens (JWT), to ensure that verifiable credentials can be easily exchanged and interpreted by different systems and services.
	Access Control and Permissions	• Define access control policies that determine who can issue, verify, and request verifiable credentials. Ensure that permissions are consistent with privacy and security requirements.
	Semantic Validation	• Implement semantic validation checks to verify that verifiable credentials conform to the defined schema and vocabulary, reducing the risk of data errors and inconsistencies.
	User-Friendly Display & Print	• Develop user interfaces that present verifiable credentials in a user-friendly format, ensuring that individuals can easily understand and manage their digital credentials and allowing export in printable versions.
Legal requirements	**Intellectual Property Rights**	• Copyright for content and materials.
	Accessibility	• Platform must be accessible to learners with disabilities in accordance with European accessibility laws.
	Accreditation and Recognition	• Educational institutions and issuers are accredited or recognized by the relevant national or regional authorities. This ensures that issued degrees and certificates have legal value.
	Data Protection (e.g. GDPR)	• Data must be handled in compliance with GDPR, including obtaining informed consent and ensuring data security.
	Consumer Protection	• Students have rights as consumers, including the right to clear information about courses and fees.

5. Interoperability Requirements

Interoperability is a crucial factor especially in the field of digital services where many different projects, standards, visions, use cases, etc., are in place. Interoperability describes the ability of different systems, software, components to interact efficiently with each other such as when they exchange data, provide services, etc. These requirements ensure that separate systems can communicate, exchange data, and function together. The section below describes the interoperability requirements that are the specifications, standards, and conditions that must be met for different systems, software, or components, libraries to work together effectively.

5.1. Technical Interoperability

Diplomasafe will expose a RESTful API service to ensure effective machine2machine communication between DS and any Partner with the wish to integrate directly with DS. Likewise Diplomasafe establishes a gateway through which DS can consume partners' offerings of interoperability such as RESTful APIs (but not limited to).

A RESTful API is a type of API that follows the principles of Representational State Transfer (REST), a software architectural style that defines a set of constraints for creating web services. A RESTful API provides a uniform and standardised way of accessing and manipulating resources on a server using HTTP methods, such as GET, POST, PUT, DELETE, and PATCH.

A resource can be any data or functionality that the server exposes to the client, such as a user, a product, a document, or a transaction. Each resource is identified by a unique URI, which is a string of characters that specifies the location and name of the resource. A RESTful API also uses a common data format, such as JSON (or XML), to represent the state and attributes of the resources in the requests and responses.

- It is simple and easy to understand, as it relies on the existing features and **standards of the HTTP protocol**, such as URIs, methods, headers, and status codes.
- It is **scalable and performant**, as it supports caching, load balancing, and stateless communication between the client and the server.
- It is **flexible and extensible**, as it allows different data formats, media types, and hypermedia links to be used for representing and linking resources.
- It is **interoperable** and platform-independent, as it enables **communication and integration among different systems**, applications, and devices, regardless of the programming languages, operating systems, or hardware they use.

5.2. Semantic Interoperability

An advantage of the MCEU Hospitality project's online platform is that it facilitates semantic interoperability among the various stakeholders and entities that participate in the micro-credential ecosystem. With Semantic interoperability the platform can ensure that the data and information that are shared among the participants have the same meaning and interpretation, regardless of the formats, languages, or terminologies they use.

To achieve this, the platform supports the use of common available standards, such as (but not limited to):

- **Europass Digital Credentials**: A set of technical standards for issuing, storing, and verifying digital credentials in a secure and verifiable way, aligned with the European Qualifications Framework (EQF) and the European Credit System for Vocational Education and Training (ECVET).
- **EDC Metadata Schema:** A metadata schema that defines the essential elements and attributes of a digital credential, such as the issuer, the recipient, the learning outcomes, the assessment methods, the level, the credit points, and the validity period.
- **European Skills, Competences, Qualifications and Occupations (ESCO):** A multilingual classification of European skills, competences, qualifications, and occupations, that enables the comparison and recognition of skills and qualifications across countries and sectors.

5.3. Legal Interoperability

One of the main benefits of the MCEU Hospitality project's online platform is that it enables legal interoperability between different actors and entities involved in the micro-credential ecosystem. Legal interoperability refers to the ability of the platform to comply with the existing legal frameworks and standards that regulate the issuance, verification, and recognition of micro-credentials in the European context. This means that the platform respects the rights and obligations of the following stakeholders:

- **DS**: The platform provider and technical partner of the project, responsible for ensuring the security, privacy, and reliability of the platform, as well as facilitating the integration with other systems and applications.
- **Credential earners**: The learners who complete the micro-credential courses offered by the project partners and receive a digital certificate that attests their skills and competences.
- **Credential issuers**: The project partners who design, deliver, and assess the micro-credential courses, as well as issue the digital certificates to the credential earners, using the platform's features and functionalities.
- **Third-party credential viewers**: The employers, educational institutions, or other organisations that access and verify the digital certificates issued by the project partners, either through the platform's interface or via an external application.

Legal interoperability covers aspects such as data protection, intellectual property, consent, liability, and dispute resolution, among others. For instance, legal interoperability ensures that:

- The platform complies with the **GDPR** and protects the personal data of the credential earners, issuers, and viewers, as well as their rights to access, rectify, erase, restrict, or object to the processing of their data. It also provides users with their data in a standardised, commonly used, and machine-readable format. This allows users to easily move their data between different services.
- The platform respects the **intellectual property rights** of the credential issuers and earners, as well as the third-party credential viewers, regarding the content, design, and format of the micro-credential courses and certificates, as well as the use and reuse of the platform's resources and services.
- The platform obtains the consent of the credential earners, issuers, and viewers, regarding the collection, storage, sharing, and verification of their data and credentials, as well as the terms and conditions of using the platform and its features.
- The platform defines the roles and responsibilities of the credential earners, issuers, and viewers, as well as the platform provider, regarding the quality, validity, and recognition of the micro-credentials, as well as the potential risks, damages, or disputes that may arise from using the platform or its services.
- The platform provides mechanisms and procedures for resolving any conflicts or complaints that may occur between the credential earners, issuers, viewers, or the platform provider, in a fair and transparent manner.

By following the best practices and EU regulations, the platform fosters trust and confidence among its users and partners, as well as facilitates cross-border mobility and employability of learners. Legal interoperability also supports the development of a common European framework for micro-credentials, which aims to enhance the transparency, recognition, and portability of credentials across different sectors, countries, and contexts.

5.4. Organisational Interoperability

Organisational interoperability refers to the alignment of business processes, organisational structures, and governance models among different entities involved in issuing, revoking, and verifying micro-credentials. The MCEU Hospitality project's online platform ensures organisational interoperability by establishing clear roles and responsibilities for each stakeholder, as well as defining common workflows and procedures for credential management.

For example, the platform designates the VET providers as the issuers of micro-credentials, who are responsible for setting the learning outcomes, assessment criteria, and quality standards of each credential. The platform also assigns the role of verifiers to employers, educational institutions, or other third parties who wish to validate the authenticity and validity of a micro-credential presented by a learner. The platform enables the communication and coordination between issuers and verifiers by providing a secure and transparent verification system based on blockchain technology.

Moreover, the platform facilitates the involvement of other relevant actors, such as accreditation bodies, sectoral organisations, or national authorities, who can endorse, recognise, or regulate the micro-credentials issued by the VET providers. The platform supports the exchange of information and feedback among these actors, as well as the alignment of their expectations and requirements. By doing so, the platform fosters trust and collaboration among the diverse stakeholders within the hospitality sector, as well as across other sectors and regions.

To ensure organisation interoperability, all the entities registered in the Credentials Issuing Online Platform must be previously identified, to provide information about the entity issuing/receiving a credential. Identification metadata provides security and trust to other parties (avoiding impersonations and fraud).

In addition, it’s necessary to have an organisational structure to ensure all the information anchored there is reliable. In this way, the responsibility is delegated in regional organisations to improve trust and processes relating to the onboarding of such entities (each Member State has its own procedures).

Each organisation must provide:

- **OID/DID (Organisation Identity):** Legal Name, National registration number (e.g., VAT code), etc.
- **Accreditations**: Unique identifiers of the schemes the organisation can issue.
- **Display information:** Type of organisation (private, public, NGO, etc), display name, EU member state of incorporation,
- **Open Services:** Each entity (in case of issuers) could define a list of services to verify issue credentials or other services they provide.

6. Conclusion

The development of the MCEU Hospitality project's online platform for issuing micro-credentials marks a significant step towards advancing digital and green skills within the hospitality sector across Denmark, Iceland, and Spain.

Through meticulous analysis of user needs, user journeys, and scenarios associated with credential issuance, revocation, and verification, as well as exhaustive consideration of technical, semantic, legal, and interoperability requirements, the platform will be user-friendly, reliable, interoperable, and compliant. It will serve as a central hub for VET providers to issue micro-credentials to learners, facilitating their lifelong learning and employability.

By aligning with the European Union's recommendation on micro-credentials, the platform ensures quality, transparency, recognition, and portability of credentials, adhering to ten key principles outlined by the Council of the EU. The platform's integration with existing EU tools and infrastructures, such as the EDC, EBSI and Europass, ensures interoperability and compatibility, further enhancing its utility and value.

Overall, the MCEU platform represents a holistic solution tailored to the specific needs of VET providers and learners in the hospitality sector, embodying the European approach to micro-credentials and supporting the EU's broader objectives of fostering lifelong learning and skills development.

7. References

Council of the European Union. 2022. Council Recommendation on a European approach to micro-credentials for lifelong learning and employability. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9237-2022-INIT/en/pdf

Europass. N.d. European digital credentials for learning. European Digital Credentials for Learning-Introduction to Digital Credentials. Retrieved from europa.eu/europass/en/stakeholders/ european-digital-credentials

European Union. 2014. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Union L 257/73. Retrieved from eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014. 257.01.0073.01.ENG

European Union. 2018. Decision (EU) 2018/646 of the European Parliament and of the Council of 18 April 2018 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC (Text with EEA relevance.) Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018D0646

8. Annexes

The European standard elements to describe a micro-credential as described in the Council of the EU's Recommendation include the following mandatory and optional elements in Table 3.

Table 3: European standard elements to describe a micro-credential

Mandatory elements	Identification of the learner
	Title of the micro-credential
	Country(ies)/Region(s) of the issuer
	Awarding body(ies)
	Date of issuing
	Learning outcomes
	Notional workload needed to achieve the learning outcomes (in ECTS credits, where possible)
	Level (and cycle, if applicable) of the learning experience leading to the micro-credential (EQF, QF-EHEA), if applicable
	Type of assessment
	Form of participation in the learning activity
	Type of quality assurance used to underpin the micro-credential
Optional elements, where relevant (Non exhaustive list)	Prerequisites needed to enrol in the learning activity
	Supervision and identity verification during assessment (unsupervised with no identity verification, supervised with no identity verification, supervised online, or onsite with identity verification)
	Grade achieved
	Integration/stackability options (stand-alone, independent microcredential/integrated, stackable towards another credential)
	Further information


MCEU