Co-funded by the European Union

DC4EU project is Co-funded by the European Union's Digital Europe Programme
under Grant Agreement no. 101102611

7.3 Interop Lab Guide

Revision: v.1.0

Work package	WP 7
Submission date	02/09/2024
Deliverable lead	Sunet / Vetenskapsrådet
Version	1.0
Authors	Stefan Liström (Sunet)
Reviewers	Leif Johansson (Sunet), Paul den Hertog (SURF), Ángel Palomares Perez (Atos), Lluís Alfons Arino Martín (SGAD), Niels van Dijk (SURF), Gerd Bauer (DVSV), George Fourtounis (GRnet)

Abstract	Deliverable to give a better understanding of the goal and setup of the DC4EU Interoperability lab
Keywords	DC4EU, EUDIW, Interoperability

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	12/08/2024	1st version of the deliverable for comments	Stefan, Leif, Niels
V0.2	27/08/2024	2nd version after WP7 review.	Stefan, Lluis, Paul, Angel
V0.3	01/09/2024	3rd version after DC4EU strategic committee review	George, Gerd
V1	02/09/2024	First final version after SC approval and Coordinator approval and submission	WP1 PMO

1.1 DISCLAIMER

Project co-funded by the European Commission in the Digital Europe Programme		
Nature of the deliverable:	**R***	
Dissemination Level		
PU	Public, fully open, e.g. web	**x**
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to DC4EU project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

EXECUTIVE SUMMARY

This document describes the goal and objectives of the DC4EU interoperability lab. The main goal is to set up the different components developed by work package 7 in DC4EU (such as the credential issuer and verifier) to help pilot the education and social security use cases in the consortium. As well as enabling other stakeholders within the consortium and outside to be able to interconnect to the interoperability lab to explore and verify interoperability. It also outlines the initial findings and areas discovered as important to focus on when piloting to achieve interoperability. To achieve interoperability, it is imperative that there are open and available standards and components that are easily accessible for all parties interested in participating in the EUDIW ecosystem to test and integrate existing solutions to the new paradigm of wallets and credentials. The DC4EU interoperability lab aims to be one of those places where stakeholders can test and integrate different components to build on the solid base and extend both scope, scalability and interoperability for existing and future solutions.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

TABLE OF CONTENT

1 INTRODUCTION 7
2 INTEROPERABILITY 8
3 INTEROPERABILITY COMPONENTS 9
4 EXPLORING INTEROPERABILITY 13
5 INTEROPERABILITY LAB 20
6 FURTHER REQUIREMENTS 21
7 CONCLUSIONS 22

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

LIST OF FIGURES

FIGURE 1 SIMPLIFIED EUDIW ECOSYSTEM FROM A NATURAL PERSON POINT OF VIEW

FIGURE 2 AUTHENTIC SOURCE INTEGRATION SCENARIO 0

FIGURE 3 AUTHENTIC SOURCE INTEGRATION SCENARIO 1

FIGURE 4 AUTHENTIC SOURCE INTEGRATION SCENARIO 2

FIGURE 5 UPDATED IMAGE OF PROVIDER DISCUSSED IN DELIVERABLE D7.1 OPEN-SOURCE ARCHITECTURE

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

ABBREVIATIONS

DC4EU	Digital Credentials for Europe
EAA	Electronic Attestation of Attributes
EBSI	European Blockchain Services Infrastructure
EUDIW	EU Digital Identity Wallet
EWC	EU Digital Wallet Consortium
FIDO	Fast IDentity Online
LSP	Large Scale Pilot
OpenID4VCI	OpenID for Verifiable Credential Issuance
OpenID4VP	OpenID for Verifiable Presentations
PID	Person Identification Data
PuB-EAA	Public Body Authentic Source Electronic Attestation of Attributes
PWAW	Progressive Web Application Wallet
QEAA	Qualified Electronic Attestation of Attributes
REST API	RESTful Application Programming Interface
RFC	Request for Comments
UI	User interface
WP	Work package

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

1 INTRODUCTION

One of the goals of the Large Scale Pilots (LSP) is to test the whole EUDI reference wallet ecosystem, from issuing the wallet to the user, to incorporating personal identity information, adding additional documents, and presenting this information to service providers. This will be done within specific domains for the different LSPs. DC4EU will test the use of the EUDI wallet in the education and social security domains. [1]

The EUDI wallet ecosystem is envisioned as a multi-vendor, multi stakeholder ecosystem with many wallets (at minimum one for each of the member states). The ecosystem is not restricted to government use cases, but allows for public sector and private sector use cases. Due to these properties, we may expect a multitude of issuers, verifiers and wallets. Hence, one of the most important aspects for the digital identity wallet ecosystem to work and scale within EU and globally is interoperability. Such interoperability is not just limited to the technical interactions between the various components. The trust fabric must be set up in such a way that it is understandable and usable across sectoral and national borders.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

2 INTEROPERABILITY

To understand the purpose of the interoperability lab it is important to understand what is meant with interoperability in this context. Interoperability can be viewed in many different ways; the following description is one of those ways and will be used for the sake of comparison in this document.

Interoperability can be seen from four layers; users and services, organisation and processes, applications and information, standards and technology and then we also have governance that in some sense interacts with all four layers. All perspectives are important and without a clear understanding of each, interoperability is hard to achieve. One of the most important aspects of any of these perspectives is that they are open and public. Without open public access to these different perspective's interoperability is hard to achieve.

An example of how the layers interact can be made with e-mail. The email standards are defining both the contents of the email (e.g. the MIME protocol) and the ways we communicate to send, receive and handle emails (SMTP, POP and IMAP). The applications are the clients and servers that people and organisations build and use and the information is the data and messages in the emails. The organisation and process layer can define organisational aspects, e.g. which email system to use. From a user perspective it is about how the user experiences the chosen systems and processes within their organisation. All these layers are glued together by the global standard, DNS, ensuring that emails are sent (under normal circumstances) to the right person. Due to the fact we have an agreed global system to handle DNS we can trust the delivery of emails even though we do not know or understand who owns or handles all the different networks our email travels through to reach its destination. On the governance layer, the relevant standards are all governed globally through so called RFCs from the IETF. Operationally, the email ecosystem itself is set up as much of the internet: all email is treated equally at transport time. As soon as a message reaches its endpoint however, the local context is taken into scope and emails may get filtered, scanned, passed on or blocked, in accordance with local rules and regulations. It is the receiving end of the ecosystem that ultimately decides how to handle the incoming messages. Other aspects of email also illustrate its true interoperability: at least in theory, anybody can spin up a piece of compatible software and become a mail server. Anyone can install one of the many email clients and use their favourite email client to participate in the ecosystem. Finally, servers and client software exist for almost every platform and operating system.

Similarly the wallet and credential ecosystem is envisioned to be a globally spanning network of interconnected components and actors. Credentials can be compared to emails as the base for information exchange and the components of issuers and verifiers used by providers of authentic sources and relying parties can be seen as the email servers while the holder wallets can be seen as the email clients and finally the trust infrastructure is where the governance in regards to the ecosystem can be ensured. This is a very simplified view of the ecosystem but is meant to give a high level example of what will be more detailed in the rest of this deliverable.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

3 INTEROPERABILITY COMPONENTS

The Digital Identity Wallet ecosystem is a complex setup of many different components. The idea of the interoperability lab is to enable the possibility to test these different components with each other irrespectively of who it was that built those particular components. This section will on a high level list and briefly scope the different components and actors interesting in this context to give the reader an understanding of the components being discussed and used in the interoperability lab.

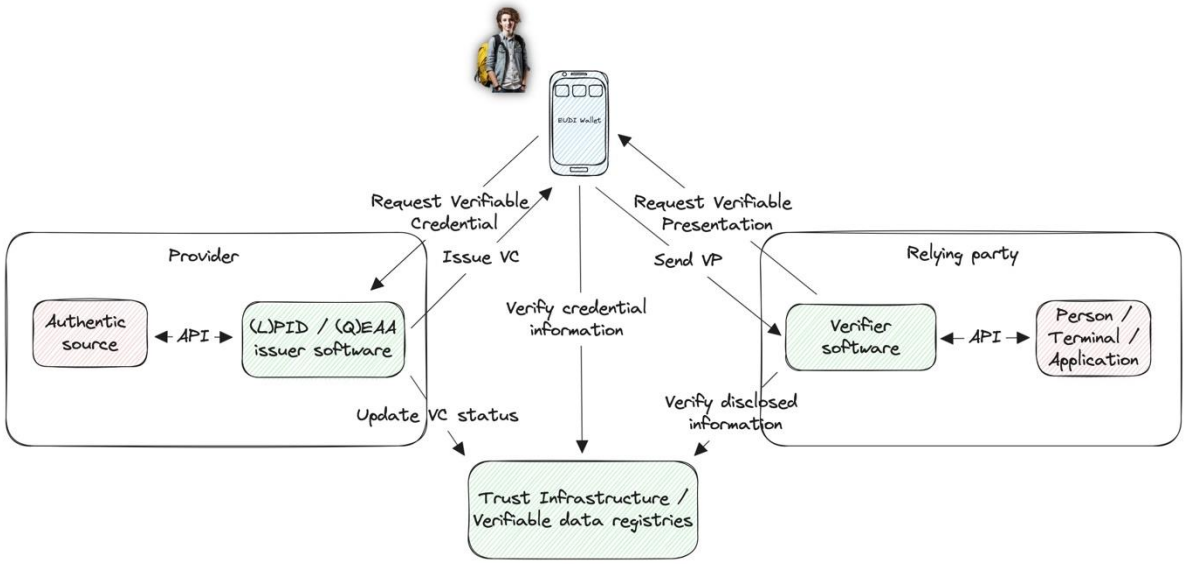

FIGURE 1 SIMPLIFIED EUDIW ECOSYSTEM FROM A NATURAL PERSON POINT OF VIEW

3.1 CREDENTIALS

There are many different names being used to refer to the collection of data or attributes that is being exchanged within the EUDIW ecosystem. In the revised eIDAS regulation [2] it is referred to as Electronic Attestation of Attributes (EAA) [3], Qualified Electronic Attestation of Attributes (QEAA) [4] and Electronic Attestation of Attributes issued by a Public Sector Body [5] (PuB-EAA in ARF [6]). In the ARF there is a distinction between an Electronic Attestation of Attributes (EAA) and Person Identification Data (PID). One of W3Cs standard drafts define the data as verifiable credentials [7] and Europass defines it as digital credentials [8].

From an interoperability point of view these are different perspectives on very similar things. That does not mean they will all be implemented technically the same. From this deliverables point of view, the term credential will be used and imply the most generalised interpretation of these definitions. If there is a need for diversification or specification it will be made clear in that particular part of the deliverable.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

3.2 AUTHENTIC SOURCE

An authentic source is a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice. [9]

3.3 ISSUER

The issuer is the software component responsible for issuing the credentials to a holder. In some cases, the issuer will be operated by the same organisation responsible for the authentic source and in other cases the issuer might be operated by another organisation on behalf of the provider of the authentic source.

3.4 HOLDER

The holder component is often referred to as a wallet. There are many ways to technically implement wallets to manage credentials. There are typically two types of wallet end-users: one is a natural person and the other is an organisational entity such as a legal person. These two types of users may have different usage and functional requirements.

Below is a non-exhaustive list of different wallet types.

Mobile Wallet Native Application
Also known as Mobile Wallet only, is an application that runs natively on a Personal Device under the sole control of an End-User and provided through a platform vendor specific app-store, on behalf of the Wallet Solution. In some cases, the End-User as a natural person uses the Mobile Wallet representing a legal person.

Web Wallet Native Application
Also known as Cloud Wallet or Web Wallet only, is a Wallet that uses native web technologies for its components, such as UI components. Cloud Wallets are typically extra suitable for Organisational Entities that require automated credential operations (request, issuance, store, presentation, revocations) in unsupervised flows, therefore without any human control. Web Wallets are divided into two additional subtypes: Custodial Web Wallets and Non-Custodial Web Wallets.

Custodial Web Wallet
Cloud Wallets that have dependency on a cloud infrastructure, not necessarily hosted by the Wallet Provider, are typically classified as Custodial Web Wallets; in this case, the cryptographic keys used and the credentials are stored in the cloud infrastructure.

Non-Custodial Web Wallet
A Web Wallet where the cryptographic keys are stored and managed on a media in possession by the End-User and the credentials can only be used by the End-User, e.g. using a FIDO enabled security hardware token, no matter whether the credentials are stored locally in a Personal Device or in cloud storage.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

Progressive Web Application Wallet (PWAW)
PWAW is a web application that looks like a native mobile app. It can be installed on a Personal Device and not necessarily using the operative system specific app-store. The advantage with a PWAW is that it gives the End-User the same experience as a Mobile Wallet Native Application while also offering the benefits of a web application. As Web Wallets the PWAW can also be Custodial or Non-Custodial.

3.5 VERIFIER

The verifier is the software component used by a relying party to verify the integrity of a credential and the trustworthiness of the provider of that credential.

3.6 RELYING PARTY

A relying party is a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service [10].

3.7 TRUST INFRASTRUCTURE

The trust infrastructure is one of the cornerstones of the EUDIW ecosystem. According to eIDAS, Member States may require the supervisory body (that shall be responsible for supervisory tasks in the designating Member State as regards trust services) to establish, maintain and update a trust infrastructure in accordance with national law [11][12].

The trust infrastructure is often also referred to as verifiable data registries. Using different registries where data can be verifiable is the foundation of the trust built into the ecosystem. Examples of such registries are entity registries, revocation registries and schema registries. There are also other aspects affecting the trust infrastructure from a business point of view that will have technical implications too, such as the attestation rule books. WP7 will in the interoperability lab primarily focus on the technical aspects but together with education and social security also further analyze how business requirements need to be taken into account to create interoperability.
One extremely important aspect of the trust infrastructure is to enable all stakeholders in the ecosystem to be able to verify the trust in each other, i.e. when exchanging information, the issuer, wallet holder and the verifier needs to be able to ensure that they can trust each other before any information is exchanged.

Entity registry
The goal of the entity registry is to have a place where all the entities participating in the exchange of credential data can be verified to help other parties decide if the data in the credential can be trusted. Some of the main entities that will likely be stored in the entity registry are the authentic source (or an issuer if they act on behalf of an authentic source), wallet providers and the relying parties. Depending on the implementation of the trust framework there can be one or more entity registries.

Status and revocation registry

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

One very important additional feature of credentials compared to many earlier forms of data exchange is the idea of being able to indicate on a global scale if they are still valid or not. This can be done in several different ways, but it is envisioned that there will most likely need to be a register where it can be verified if a certain credential is still valid, if it has been suspended or if it has been revoked. There can be several reasons for suspending or revoking a digital credential, e.g. because the user asked for it, the credential has expired or the information that was issued was found faulty.

Schema registry

To make the digital credentials understandable within (and sometimes outside) a certain domain there needs to be an agreement on how the attributes are structured in the credential, this is one of the functionalities of the schema registry. It is imperative for issuers, holders and verifiers of credentials to understand how to process the data within the credential in an interoperable way.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

4 EXPLORING INTEROPERABILITY

The DC4EU Large Scale Pilot will explore interoperability from different perspectives, such as technical, legal and semantical interoperability. Primarily the goal is to look at interoperability from a whole ecosystem point of view. This section will look at the different components in the ecosystem and view the aspects to that particular component from an interoperability point of view.

4.1 CREDENTIALS

From a credential point of view DC4EU will look at the differences and similarities between PIDs, EAAs, PuB-EAAs and QEAAs when being issued and used in the credential ecosystem. The primary focus of credentials in DC4EU are the education (educational and professional qualifications) and social security (EHIC and PD A1) domains.

4.2 AUTHENTIC SOURCE

When it comes to the authentic source (AS) there are a couple of different scenarios that are important for DC4EU to investigate and enable the piloting agents in the consortium to pilot in the education and social security use cases. Below are overviews of the scenarios to issue credentials from an authentic source in different setup.

4.2.1 Scenario 0 – AS issuing credentials

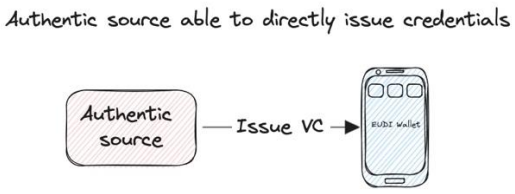

FIGURE 2 AUTHENTIC SOURCE INTEGRATION SCENARIO 0

In a future scenario authentic sources might be able to directly interface and interact with the EUDIW ecosystem to issue credentials. When the software or services used by the authentic source can support the standards needed to work natively. However as both regulations and consensus around technical standards and implementation of this ecosystem is still developing it is considered unlikely that this scenario will be feasible in the near future. Given that the DC4EU LSP has an ambitious approach within a very narrow time limit two other scenarios will be investigated within the scope of the DC4EU pilot.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

4.2.2 Scenario 1 - AS using issuer to issue credentials

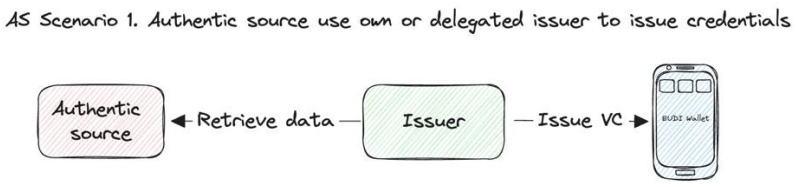

FIGURE 3 AUTHENTIC SOURCE INTEGRATION SCENARIO 1

To enable an existing authentic source to interact with the EUDIW ecosystem DC4EU will develop an open source issuer component. The goal of the issuer component is to on one hand be able to communicate with the authentic source based on current available, well tested and stable standards in regards to web technologies. That way the effort from the authentic source will be less to enable them to interact with the new developing EUDIW ecosystem. On the other hand, the issuer component will implement the standards and specifications being developed to enable interoperability in the EUDIW ecosystem, e.g. issue a credential based on the de facto agreed on standards such as OpenID4VCI.

4.2.3 Scenario 2 - AS using datastore and issuer to issue credentials

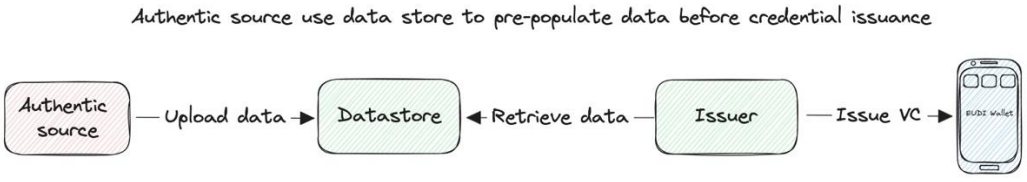

FIGURE 4 AUTHENTIC SOURCE INTEGRATION SCENARIO 2

In early discussions within DC4EU it became clear that some organisations that will participate in the piloting of the DC4EU use cases will have problems directly interconnecting with existing authentic sources to a new software component outside of their already established infrastructure. This could be for reasons where the current software used by the authentic source is using technologies or standards that are not easily made compatible with current web technologies preferred in new developments. It could also be because the current security domains for the authentic source do not easily allow for new components to interact with current established infrastructure.

To work around these concerns DC4EU will also explore a scenario where the Authentic source can upload attributes needed to create a credential into a datastore. The datastore will act as the authentic source from an information storage point of view but should not contain any of the business logic that the authentic source might have or need. The goal with this approach is to make it easier for current security standards within piloting organisations to be followed and still enable the organisation to participate in the piloting of the DC4EU use cases.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

The components needed for an authentic source to pilot scenario 1 or scenario 2 are being developed and made public by open source in the DC4EU GitHub repository [13].

4.2.4 Authentic source legal interoperability

Another interoperability aspect in regards to the authentic source that will be interesting to investigate is how the legal jurisdictions can be considered by the setup suggested by DC4EU. In other words what are the legal implications of an authentic source to issue their own credentials or outsourcing the issuing to another organisation. It is also of interest to look at the different scenarios of the owner of the certificate that is used to issue and seal a credentials, e.g. is it owned by the authentic source, the organisation issuing the credential or a remote e-seal service being used by the issuer.

4.3 ISSUER

The issuer is a very complex component and is investigated in more detail in the DC4EU deliverable D7.1 Open Source Architecture [14]. The interoperability lab deliverables will investigate more in depth the external interfaces used by the issuer. From an interoperable perspective there are three components and interfaces that are important to take note of, the interface to the authentic source, the interface to the holder wallet and the interface to the trust infrastructure.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

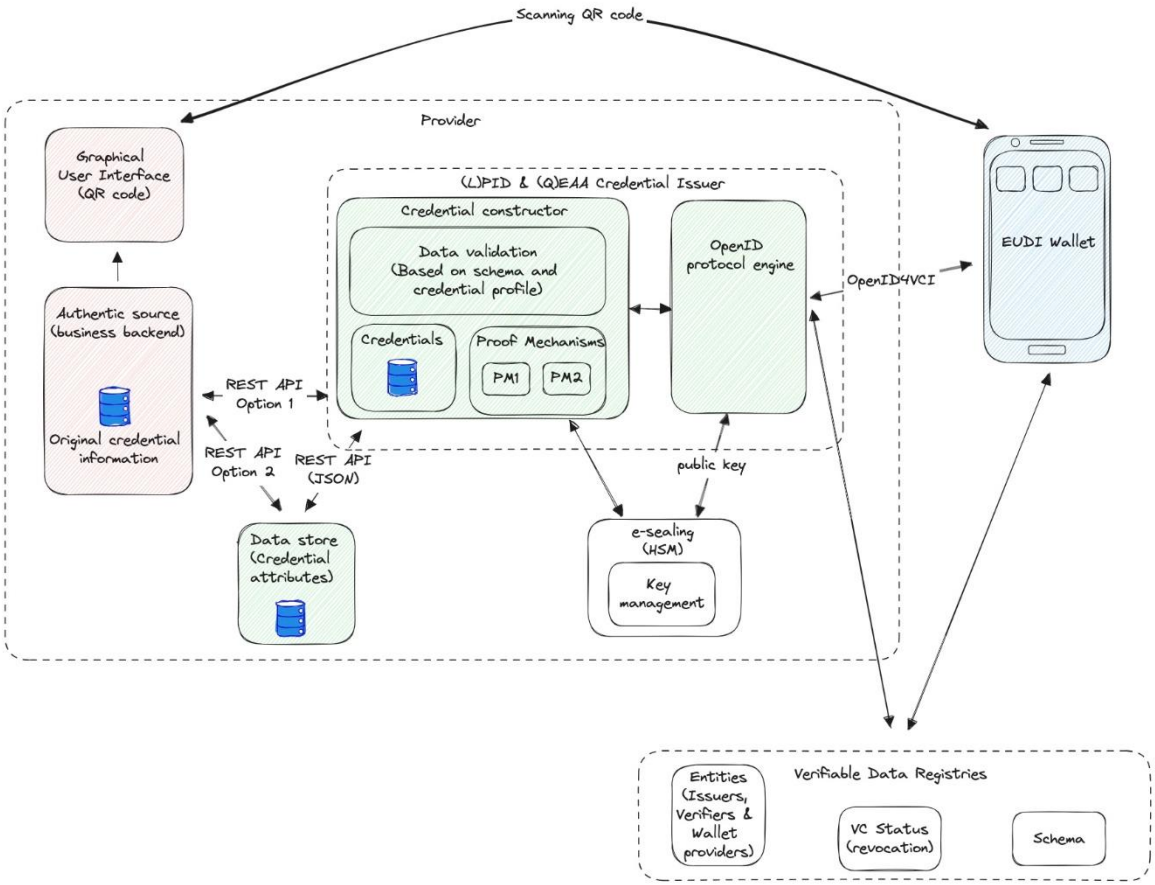

FIGURE 5 UPDATED IMAGE OF PROVIDER DISCUSSED IN DELIVERABLE D7.1 OPEN SOURCE ARCHITECTURE

4.3.1 Issuer and Authentic source

The interface between the authentic source and the issuer has already briefly been discussed in the section Authentic source under Exploring interoperability. What is relevant to add in this section is that the actual interface is a REST API, which is a very common API used for web development. The API specification is publicly available in the open source code accessible via DC4EU GitHub repository [15]. The Interoperability lab will be able to investigate if there needs to be any particular differences in regards to the interface when issuing an EAA, PuB-EAA or a QEAA.

4.3.2 Issuer and holder wallet

The interface between the issuer and the holder wallet is based on the OpenID4VCI [16] which is an agreed upon standard to use for credential issuance in the ARF. OpenID4VCI can be seen as a framework and there are many decisions that need to be made when implementing OpenID4VCI. This opens up for many different types of implementations which will make interoperability more challenging. The DC4EU LSP will define how OpenID4VCI is implemented in the DC4EU issuer and have an open dialogue with other LSPs and other

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

stakeholders regarding their choices to try to find the commonalities to achieve interoperability. The WP5 education domain requirements to use the EBSI profile shall also be taken into account.

4.3.3 Issuer and trust infrastructure

The interface between the issuer and the trust framework will most likely look different depending on which trust framework is being used. The three trust frameworks DC4EU is particularly interested in are the currently used Trusted Lists, EBSI and OpenID federation.

4.3.4 Issuer semantic interoperability

Technical interoperability is important for the issuer to be able to exchange credentials with other entities. However, another very important interoperability aspect is the semantic interoperability. The issuer needs to be aware of how to semantically structure the credentials in an agreed way so that they will be able to be processed at a later stage by entities either verifying the credential or consuming the attributes within the credential. It is also important for the issuer to be aware of how to structure the attributes within the credential so that they can be selectively disclosed by the end user in a way that the authentic source has agreed on. This semantic interoperability information can be stored in a schema that can be used both by the issuer but also the verifier.

The work done in WP5 education creating converters between e.g. ELMO and ELM and also looking into Microcredentials and Openbadges can be a useful tool to help contribute to semantic interoperability.

4.4 HOLDER

The holder is the one component with the most external interfaces and complex relationships to other parts of the ecosystem.

Natural person
When the end user of the holder wallet is a natural person it is expected that the interface between the end user and the holder wallet is a graphical user interface used most times either in a mobile phone or on a laptop. This deliverable will not go into detail regarding the interoperability of the graphical user interface but there are a lot of interesting topics that could be evaluated during the pilot. Particularly the potential conflict of the wallet ecosystem giving the user control of their own data but also trying to protect the user from sharing this data with the “wrong” entities.

Legal person
The end-user of the holder wallet could be a legal person, but as that is not the main use case within DC4EU this will not be explored in detail in this deliverable. Even though it is not a priority to investigate this aspect within DC4EU it is still being considered as an important part of enabling the complete ecosystem.

Holder and issuer
The holder needs to be able to verify trust towards the issuer before receiving credentials. How this can be achieved is suggested in the ARF and is also expected to be defined in the eIDAS

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union’s Digital Europe Programme under Grant Agreement no. 101102611

implementing acts. This is certainly one aspect that DC4EU will also investigate when looking at the interoperability between the entities in the EUDIW ecosystem.

Holder and verifier
The holder needs to verify trust towards the verifier before sending a presentation. This process is expected to be similar to the holder verifying the trust towards the issuer.

4.5 RELYING PARTY

The relying party has two interfaces that are important to ensure they are interoperable. The main one towards the verifier. Depending on who the relying party is, the interface might have different requirements. The relying party could be a person, a software application or a physical device that is used to e.g. receive a credential presentation over NFC.

The second interface that is of importance to the relying party is the external interface towards the trust infrastructure to be able to onboard and update information regarding the relying party.

4.6 VERIFIER

The verifier has similar interoperability interfaces as the issuer. The difference is that instead of OpenID4VCI the verifier should interface with the holder wallet using OpenID4VP [17].
The interface from the verifier software used by the relying party is planned to be a REST API to easily enable other software to interface with the verifier and verify credentials as well as extract the information from the credentials if the data should be processed.

The interface between the verifier and the trust infrastructure is very similar to the issuers interface towards the trust infrastructure. The verifier needs to be able to verify the validity of the wallet instance as well as the trust in regards to the provider of the credential presented towards the trust infrastructure. The verifier also needs to be able to look up or already understand the schema of the credential to be able to extract and make sense of the information inside the credential.

4.7 TRUST INFRASTRUCTURE

The revised eIDAS regulation defines a collection of rules for the European member states that ensure the legitimacy of the components and the entities involved in the EUDI Wallet ecosystem. Within that trust model there is a possibility for several different trust infrastructures to operate. Within DC4EU we will explore three of the possible candidates for trust infrastructures available. The first is the already existing trust infrastructure used in the current eIDAS federated identity system called Trusted lists and Lists of Trusted lists [18]. The second trust infrastructure that is interesting for DC4EU is a Decentralized Public Key Infrastructure (DPKI) such as EBSI [19]. The third trust infrastructure DC4EU will look into is OpenID federation [20].

Trusted lists and Lists of Trusted lists

The trusted lists trust infrastructure is an already proven method of creating trust within the eIDAS system so will not be investigated to any great length within the project but

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

still is an important part of the ecosystem so it will have a part in the interoperability lab. One of the expected challenges with the lists of trusted lists infrastructure is scalability in the revised eIDAS ecosystem when there will be a multitude more entities represented in the trust infrastructure as both providers of credentials, wallet providers and relying parties will most likely have to be recorded in the trust infrastructure to achieve the extended trust model envisioned in the eIDAS regulation. This is one of the reasons why DC4EU is also investigating other trust infrastructures.

Decentralized Public Key Infrastructure - EBSI
From the beginning of the DC4EU LSP EBSI has been a part of the trust infrastructures that the LSP would like to explore and pilot. The integration and use of EBSI in the DC4EU LSP is closely detailed in the educational business blueprint deliverable (D5.1 – Business Blueprint WP5). The interoperability lab will investigate how this can be implemented in the best possible way.

OpenID federation
OpenID Connect is one of the foundational standards when it comes to the envisioned credential ecosystem described by the ARF as both OpenID4VCI and OpenID4VP are the standards used for issuing and presenting credentials. OpenID Federation has many similarities with the OpenID Connect standards and is looking to be a very interesting candidate for a functional and scalable trust infrastructure.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

5 INTEROPERABILITY LAB

To explore the different kinds of interoperability explained in this deliverable, DC4EU is setting up what is called an interoperability lab. The EUDIW ecosystem is a complex mix of many different roles and components to achieve the end result of being able to exchange credentials across organisations, national borders as well as cultural and domain contexts. The goal of the DC4EU interoperability lab is to enable a space for these many roles and components to explore what is needed for all of them to work together in an interoperable way.

The DC4EU strategy to achieve this is to initially setup the core components by the LSP. Once the initial components are available and interconnected the interoperability lab will open up for other partners and possibly external stakeholders to interconnect to the Interoperability lab too.

The authentic sources will initially consist of the stakeholders in the DC4EU domains of WP5 education and WP6 social security.

The issuer and verifier will initially consist of the software components being developed within WP7.

The trust infrastructure used will be the already existing setup of EBSI nodes and a setup of OpenID Federation that WP7 will develop and deploy.

The holder wallet will initially be the wallets within the DC4EU consortium as well as the Reference Implementation, later in the pilot the interoperability lab will open up for interoperability testing with other external wallets too.

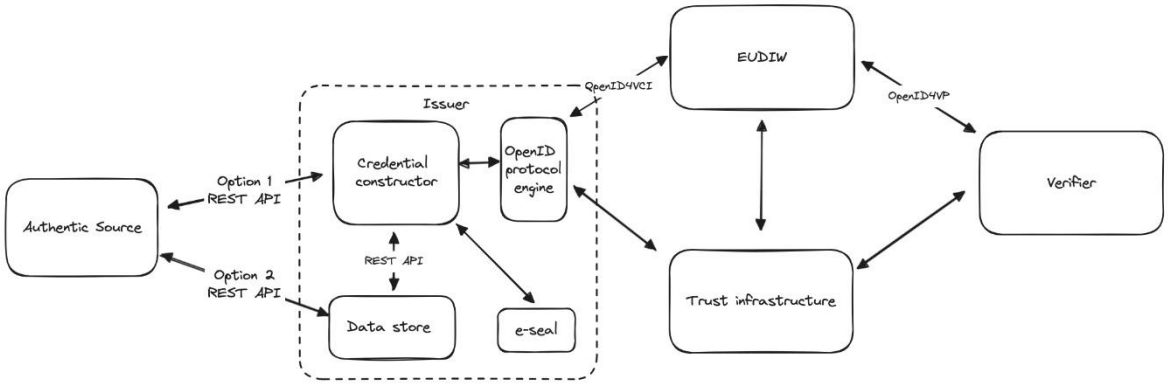

FIGURE 6 INITIAL INTEROPERABILITY SETUP

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

6 FURTHER REQUIREMENTS

6.1 EDUCATION REQUIREMENTS

The main requirements for education for the interoperability lab comes from the DC4EU WP5 education work package deliverable D5.1 – Business Blueprint WP5. At the time of writing this deliverable the D5.1 deliverable is still in review and will not be covered in detail in this deliverable.

6.2 SOCIAL SECURITY REQUIREMENTS

The main requirements for social security for the interoperability lab comes from DC4EU WP6 social security work package deliverable D6.1 – Business Blueprint WP6 that has recently been published. As the main use cases and requirements are very well formulated in the deliverable they will not be covered in detail in this deliverable.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

7 CONCLUSIONS

This deliverable outlines the main components envisioned in the EUDIW ecosystem that the DC4EU LSP intends to explore while testing and piloting interoperability between the EUDI wallets and other components needed to fulfill the revised eIDAS regulation. This will in part be done by building an interoperability lab where DC4EU and other stakeholders can explore how different components in the ecosystem can work together despite being built and hosted by different organisations.

Going further the interoperability lab will be an excellent way to understand how the wallet and credential ecosystem can continuously be innovated while at the same time ensuring that future revisions of the development can still maintain interoperability with the existing infrastructure being developed and put in production around the world.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

REFERENCES

[1] https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20240520

[3] eIDAS (see reference [2]) Article 3 point 44

[4] eIDAS (see reference [2]) Article 3 point 45

[5] eIDAS (see reference [2]) Article 3 point 46

[6] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/#36-public-body-authentic-source-electronic-attestation-of-attributes-pub-eaa-providers

[7] https://www.w3.org/TR/vc-data-model-2.0/

[8] https://europass.europa.eu/en/what-are-digital-credentials

[9] eIDAS (see reference [2]) article 3 point 47

[10] eIDAS (see reference [2]) article 3 point 6

[11] eIDAS (see reference [2]) article 46b point 1

[12] eIDAS (see reference [2]) article 46b point 5

[13] https://github.com/dc4eu/

[14] https://dm158x9fyyzgp.cloudfront.net/wp-content/uploads/2024/02/DC4EU_D7.1_Open-Source-Architechture_v2.1.pdf

[15] https://github.com/dc4eu/vc/tree/main/standards

[16] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[17] https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[18] https://portal.etsi.org/TB-SiteMap/ESI/Trust-Service-Providers

[19] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home

[20] https://openid.net/specs/openid-federation-1_0.html

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611