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

D7.1 Open-Source Architecture

Revision: v.1.0

Work package	WP 7
Task	T7.2. Opensource Provider and Verifier
Submission date	28/12/2023
Deliverable lead	Sunet
Version	2.1
Authors	Stefan Liström (Sunet), Leif Johansson (Sunet)
Reviewers	Lluís Alfons Ariño Martín (SGAD), Peter Eikelboom (SIDN), Ángel Palomares Perez (ATOS)

Abstract	Document exploring the architecture for the open source issuer and verifier components built by work package 7 in DC4EU.
Keywords	DC4EU, Issuer, Verifier, ARF

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

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	30/10/2023	1st version of the deliverable for comments	Peter Eikelboom (SIDN), Ángel Palomares Perez (ATOS)
V2.0	21/12/2023	2nd version after internal feedback	Lluís Alfons Ariño Martín (SGAD)
V2.1	28/12/2023	Internal approval & quality check	COO PMO (SGAD)

DISCLAIMER

COPYRIGHT NOTICE

Project co-funded by the European Commission in the Digital Europe Programme		
Nature of the deliverable:	**R, document**	
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 outlines the open-source architecture that is expected to be built and tested in the DC4EU Large Scale Pilot (LSP). The goal of this document is to give stakeholders an overview of the plans made in Work Package 7 (WP7), Task 7.2. Opensource Provider and Verifier in DC4EU. Due to the many different factors that are under change and affecting the current digital identity wallet ecosystem it is expected that these plans will change over the course of the pilot. This document should therefore be seen as an initial snapshot of how the architecture could be built and can also be used as a foundation for further discussions around the architecture as such. Going forward the architecture will be continually updated in an iterative process based on the external factors to the LSP that become more clear, external factors such as the revision of the eIDAS regulation, updates to the Architectural Reference Framework and other standardisation efforts that affect the EUDI wallet eco-system.

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 CONTENTS

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

IP	Internet Protocol
TCP	Transmission Control Protocol
ARF	Architectural Reference Framework
API	Application Programming Interface
CA	Certificate Authority
DC4EU	Digital Credentials for EU
EAA	Electronic Attestation of Attributes
eIDAS	electronic identification and trust services
EHIC	European Health Insurance Card
EUDIW	European Digital Identity Wallet
HSM	Hardware Secure Module
LoA	Levels of Assurance
OpenID4VCI	OpenID for Verifiable Credential Issuance
OpenID4VP	OpenID for Verifiably Presentation
PDA1	Portable Document A1
PID	Personal Identification Data
REST	Representational State Transfer
QEAA	Qualified Electronic Attestation of Attributes
QES	Qualified Electronic Signature
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trusted Service Provider

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. SCOPE

The EUDIW ecosystem contains many different components and actors. This report will primarily take the same perspective of the ecosystem as the Architectural Reference Framework (ARF) [1] that the eIDAS-toolbox group presents, as this is the foundation for the technical interoperability discussions for all four EUDIW large scale pilots. From this perspective the report will go into details regarding the provider (issuer) and the relying party (verifier) as those are the main architectural components that WP7 - Integrations and development in DC4EU are responsible for.

1.1 OUT OF SCOPE

There is currently no official task in WP7 that is focusing on the digital identity wallet itself. As such this report will not go into details regarding the design or architecture of the digital identity wallet. However, once the reference implementation [2] of the wallet will become available to DC4EU it will be an iterative process to use and test the reference wallet with the components built in WP7.

The design of the Verifiable Data Registries will be out of scope for this report. The Interoperability lab deliverable in WP7 will go into more detail regarding this topic. Once Work Package 5 (Education) and Work Package 6 (Social Security) in DC4EU are ready with their business requirements more details about registry integration will be added to the architecture of WP7 components.

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. EUROPEAN DIGITAL IDENTITY WALLET ECOSYSTEM

2.1 ARCHITECTURAL REFERENCE FRAMEWORK

On 3 June 2021, the European Commission adopted a Recommendation calling on Member States to work towards the development of a Toolbox including a technical Architecture and Reference Framework (hereinafter the ARF), a set of common standards and technical specifications and a set of common guidelines and best practices.

The eIDAS Expert Group has since further developed the concepts and specifications for the European Digital Identity Framework based on the Commission's legislative proposal, and will continue to do so until the legislative negotiations have been concluded and implementing acts have been adopted.

The DC4EU LSP will closely follow the iterative development of the ARF as that will be a fundamental part of ensuring interoperability between the outputs from DC4EU and other LSPs. The work in DC4EU WP7 will in particular follow, update and align the architecture to changes in the meaning of roles such as Authentic source, Provider and Public sector body.

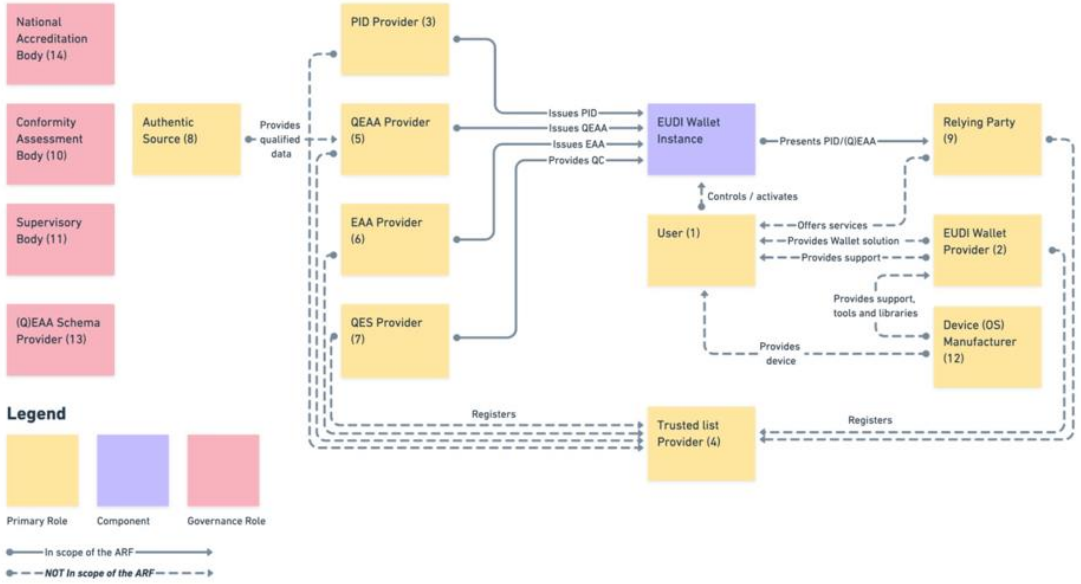

Figure 1. EUDIW ecosystem described in the ARF v1.0

Figure 1 shows the EUDIW ecosystem from the ARF point of view. Most interesting for this report are the roles Authentic source, providers and the Relying party. This report will briefly also outline the trusted list provider component. The mentioned roles are explained below according to the ARF definitions.

2.2 AUTHENTIC SOURCES

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

Authentic Sources are the public or private repositories or systems recognised or required by law containing attributes about a natural or legal persons. The Authentic Sources in scope of Annex VI of the legislative proposal are sources for attributes on address, age, gender, civil status, family composition, nationality, education and training qualifications titles and licences, professional qualifications titles and licences, public permits and licences, financial and company data. Authentic Sources in scope of Annex VI are required to provide interfaces to QEAA Providers to verify the authenticity of the above attributes, either directly or via designated intermediaries recognised at national level. Authentic Sources may also issue (Q)EAA-s themselves if they meet the requirements of the eIDAS Regulation. It is up to the Member States to define terms and conditions for the provisioning of these services, but according to the minimum technical specifications, standards, and procedures applicable to the verification procedures for qualified electronic attestations of attributes.

2.3 PERSON IDENTIFICATION DATA (PID) PROVIDERS

PID Providers are trusted entities responsible to:

- verify the identity of the EUDI Wallet User in compliance with LoA High requirements,
- issue PID to the EUDI Wallet in a harmonised common format and make available information for Relying Parties to verify the validity of the PID.

The terms and conditions of these services are for each Member State to determine.

PID Providers may e.g., be the same organisations that today issue official identity documents, electronic identity means, EUDI Wallet Providers etc. EUDI Wallet Providers may or may not be the same organisations as PID Providers.

2.4 QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES PROVIDERS

Qualified EAA are provided by QTSPs. The general Trust Framework for QTSPs apply also to QEAA, but specific rules for this Trust Service need to be defined as well. QEAA Providers maintain an interface for requesting and providing QEAAs, including a mutual authentication interface with EUDI Wallets and potentially an interface towards Authentic Sources to verify attributes. QEAA Providers provide information or the location of the services that can be used to enquire about the validity status of the QEAAs, without having an ability to receive any information about the use of the attestations. The terms and conditions of these services are for each QTSP to determine, beyond what is specified in the eIDAS Regulation.

2.5 NON-QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES PROVIDERS

Non-qualified EAA can be provided by any Trust Service Provider. While they are supervised under eIDAS, it can be assumed that other legal or contractual frameworks than eIDAS mostly govern the rules for provision, use and recognition of EAA. Such other frameworks may cover policy areas such as driving licences, educational credentials, digital payments, although they may also rely on qualified Electronic Attestation of Attributes Providers. For EAA to be used,

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

TSPs offer Users a way to request and obtain EAA, meaning they need to technically comply with EUDI Wallet interface specifications. Depending on the domain rules, EAA providers may provide validity information about EAA, without having an ability to receive any information about the use of the EAA. The terms and conditions of issuing EAAs and related services are subject to sectoral rules.

2.6 QUALIFIED AND NON-QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURE/SEAL PROVIDERS

Article 6a(3) of COM(2021)281 final requires the EUDI Wallet to enable the User to create qualified electronic signatures or seals. This goal can be reached by several ways:

- The EUDI Wallet is certified as a qualified signature/seal creation device (QSCD), or
- It implements secure authentication and signature/seal invocation capabilities as a part of a local QSCD or a remote QSCD managed by a QTSP.

2.7 RELYING PARTIES

Relying Parties are natural or legal persons that rely upon an electronic identification or a Trust Service. In the context of EUDI Wallets, they request the necessary attributes contained within the PID dataset, QEAA and EAA from EUDI Wallet Users to rely on the EUDI Wallet, subject to the acceptance by the owner of the Wallet (User) and within the limits of applicable legislation and rules. The reason for reliance on the EUDI Wallet may be a legal requirement, a contractual agreement, or their own decision. To rely on the EUDI Wallet, Relying Parties need to inform the Member State where they are established and their intention for doing so. Relying Parties need to maintain an interface with the EUDI Wallet to request attestations with mutual authentication. Relying Parties are responsible for authenticating PID and (Q)EAA.

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. OVERVIEW AND INTEROPERABILITY

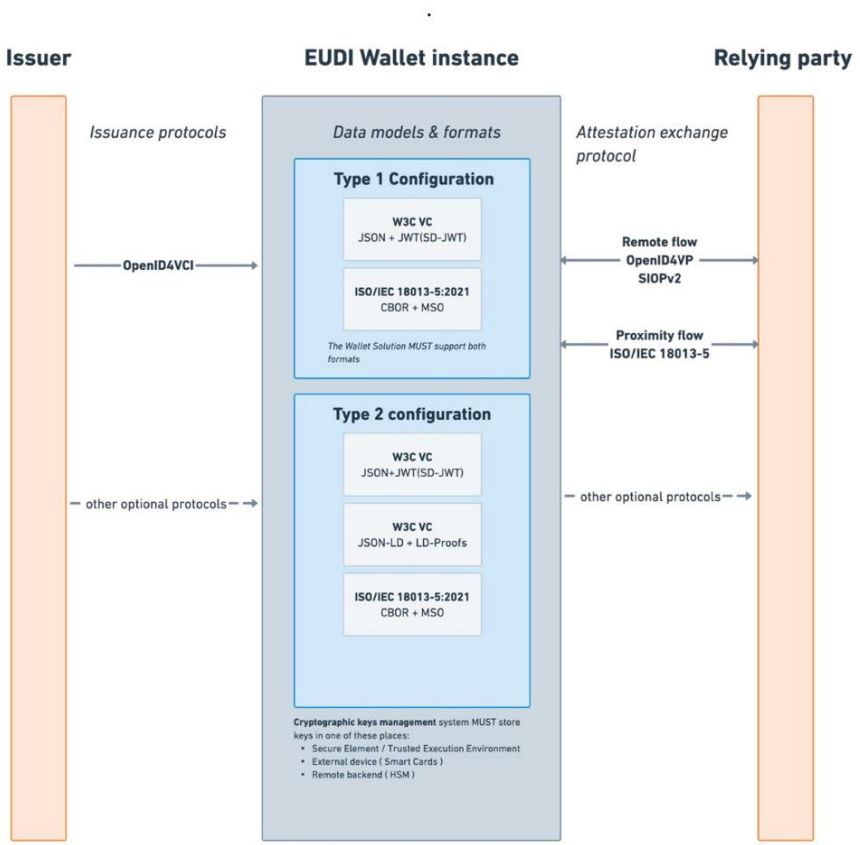

Figure 2: EUDIW configuration as specified in ARF v1.0

Figure 2 shows the different configurations of Digital Credentials an EUDIW can contain. What is most interesting for the sake of this report is the interfaces from the issuer to the EUDIW and from the EUDIW to the relying party. This will be further explained in the issuer and verifier sections in this report.

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

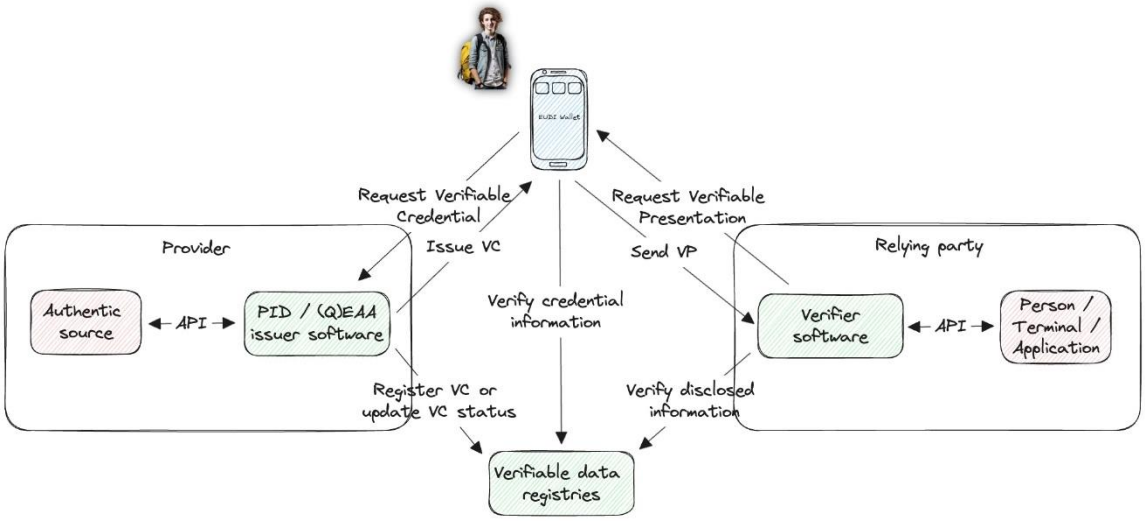

Figure 3: Simplified EUDIW ecosystem

The above simplified EUDIW ecosystem depicts the main components and roles interesting for this report and the relationship between them.

To achieve interoperability within the EUDIW ecosystem both nationally and internationally the different components and actors need to be able to communicate with each other even though the systems used are built by different organisations and acting within different countries. One way to achieve such interoperability is to agree on a set of standards to use both for formatting of information passed in the ecosystem and for the communication between components within the ecosystem. In the EUDIW ecosystem it is the ARF that defines those standards. The standards decided on within the EUDIW ecosystem are fairly new standards which means that many of today's already existing IT-infrastructure are not using those standards yet.

To achieve wide adoption and make the EUDIW a success it is therefore considered within DC4EU that it is very important to help the current IT-infrastructure that has potential to benefit of the EUDIW to be able to use the standards suggested in the ARF. New infrastructure that will be built once the EUDIW ecosystem is in place might support the necessary standards from the start. But much of the current IT-infrastructure is not aligned with the decided standards and the easiest way to help them is to build freely available and easy to use software that enables current infrastructure to communicate with the new EUDIW ecosystem.

In DC4EU there are three components that are considered critical to get existing IT-infrastructure compliant with the EUDIW ecosystem as quick as possible.

The first is a PID and (Q)EAA issuer software, called issuer from here on. An authentic source can connect to the issuer using a bidirectional API based on existing widely adopted standards and then allow the issuer to package the authentic source information (attributes) in a way that is compatible with the standards in the ARF and communicate with other entities within the EUDIW ecosystem.

The second component is a verifier software, called verifier from here on. The verifier helps the relying party that needs to receive and interpret information from the EUDIW ecosystem

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

to do so without having to implement the ARF standards in their current IT-infrastructure. With the DC4EU solution the relying party will be able to connect current infrastructure to the verifier's APIs and then easily communicate with the rest of the EUDIW ecosystem.

The third component is the different Verifiable Data Records necessary in the ecosystem to generate trust. However, the design of Verifiable Data Records is primarily outside the scope of this report. WP7 will be integrated into the verifiable data records deemed necessary within DC4EU, at a minimum the instantiation of records in EBSI will be take into consideration for this purpose.

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. PROVIDER

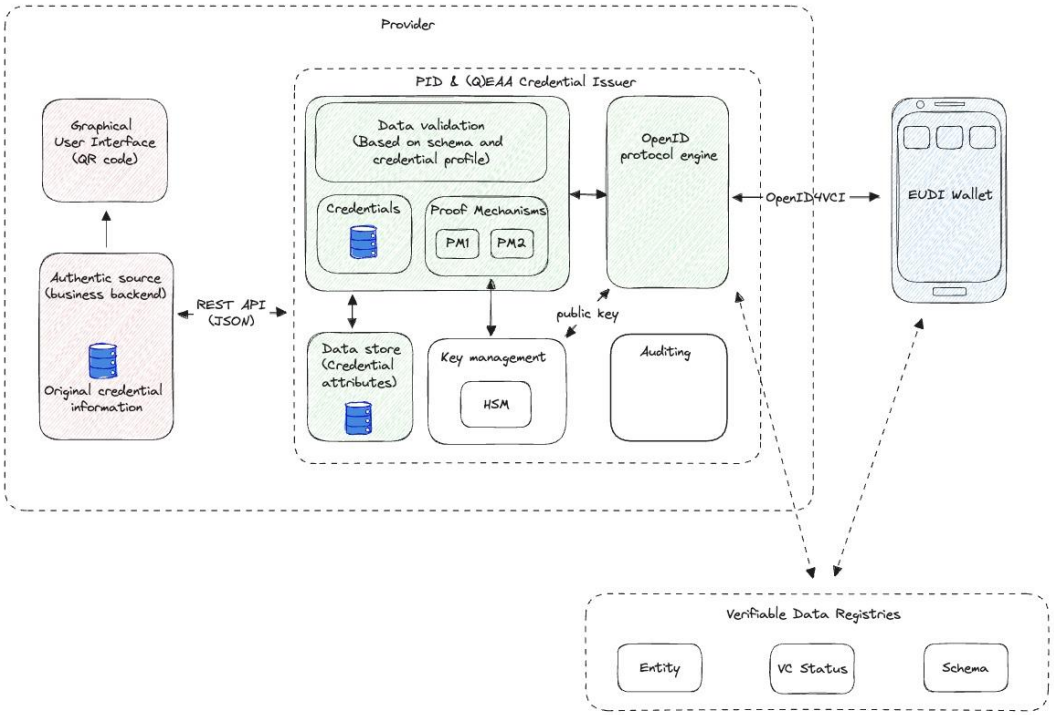

Figure 4: Provider architecture suggestion

From the provider of credentials point of view there are a couple of aspects that need to be taken into account to be able to issue credentials to the EUDIW ecosystem. As already mentioned there will most likely be some time before an authentic source IT-infrastructure is updated and natively support all the protocols and standards that the EUDIW ecosystem requires. Until then there will be complementary software or services that enable already existing authentic sources to interact with the EUDIW ecosystem.

In this chapter the report will give a suggestion on how the architecture of a supporting application or service could be built to allow an authentic source to interface with the EUDIW ecosystem by defining certain components that would be useful.

4.1 AUTHENTIC SOURCE

The Authentic source represents the organisation and the data that an organisation wants to use to create Credentials to release to a wallet, e.g. a (Q)EAA or a PID. There will most likely be a different authentic source for every use case. In DC4EU we are piloting the educational and social security use cases. In education the goal is to pilot how to request, issue, receive, store, and verify educational credentials and professional qualifications in the wallet. From the social security use case DC4EU will pilot how to issue, store, request, receive and verify the PDA1 and EHIC credentials in the wallet.

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

In some instances the authentic sources are one single organisation acting as their own issuer of digital credentials. But in other cases several authentic sources could have delegated the role of acting as their issuer of credentials to another organisation. How this will work practically in regard to the owner of the certificates used will have to be investigated during the pilot. The goal of the WP7 components are to be configurable so that several use cases can be supported This is why the supporting software needs to be scalable and both be able to run within one organisation but also run as a service where one organisation is acting on behalf of many authentic sources.

The idea is that the authentic source will communicate with the issuer using a REST API where the content sent is formatted in JSON.

4.2 GRAPHICAL USER INTERFACE

In many use cases where an authentic source wants to issue a credential to a wallet the user holding that wallet will first be in contact with the authentic source to select which credential they would like to be generated to then be able to receive it into their wallet.

This process will often start by the user accessing the webpage of the organisation that is responsible for a particular authentic source. In this webpage the user will be able to select which credential they would like to have issued and the webpage will be able to (in connection with the authentic source and issuer) present a QR-code to the user. This QR-code can be scanned by a user's wallet to initiate a flow where the wallet retrieves the credential from the issuer.

The above is only one example flow. The business blueprints from Education (WP5) and Social Security (WP6) are expected to bring forward other use flows that will be investigated by WP7 during the pilot.

4.3 CREDENTIAL ISSUER

In many cases an organisation or authentic source do not have the capability to adapt their legacy systems directly to issue Credentials to an EUDI wallet or be compliant with related security and legal measures and procedures. If that is the case, they can use a software that have APIs both towards the business legacy systems and APIs towards the EUDI wallets.

4.4 DATA VALIDATION

It is very important that the data in the issuer is both correct and understood by the issuer, from that perspective there will be a need for different kinds of data validation. The data coming from the authentic source needs to be validated that it is from a trusted party but also correctly formatted and structured. In a similar fashion the data needs to be validated by the issuer before it is issued as a credential to a wallet or the trusted registries.

To make sure that there is a clear understanding of the attributes in the credential between the authentic source, issuer and verifier there needs to be a defined and agreed on schema

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

that the issuer is aware of. The schema will most likely be different based on the credentials and use case involved. Another potential benefit of the schemas is to enable a way to agree on selective disclosure between providers and relying parties.

To achieve interoperability between all components in the wallet ecosystem the issuer most likely needs to take into account that there might exist different trust infrastructures in different member states or different contexts that e.g. are not standardized within the ARF. As such, the issuer system we will build in DC4EU has the goal of being able to accommodate for different types of credential profiles. WP7 will initially look at implementing two profiles, one will be EBSI and the other current alternative being looked at is SD-JWT-VC. The following two data sources are listing a few of the credential profiles that are being worked on within the wallet ecosystem; Google docs [3] and Github [4]. To explore how it works using different credential profiles the goal is to implement two profiles within the DC4EU pilot, see ANNEX I. For more detailed information it is possible to read more about the two profiles that are expected to be implemented in the Google docs linked above. In the referenced information the profiles are called SD-JWT-VCs (row 12) and ESSIF (row 16).

4.5 CREDENTIALS

In most cases the issuer (rather than the authentic source) will be the component that keeps track of credentials that have been issued. The main reason for this is to enable traceability but also the possibility for revoking or suspending a certain (or several) credentials at a later stage. This process will need to be tracked by the issuer as evidence in the future. It should be noted though that it will always be a business decision taken by the source to revoke or suspend the credential even though it might be the issuer that technically performs the task.

4.6 PROOF MECHANISMS

Depending on the credential profile used the proofing mechanism might look different. Both from a signature point of view but also differences in regard to the trust framework being used. Due to the fact that the revision of the eIDAS regulation is not done yet there are still several questions that are open when it comes to e-signatures and e-seals in regard to the roles of QTSP, QTS and QSCD in the wallet ecosystem. WP7 intends to investigate and hopefully be able to clarify these aspects during the pilot and suggest implementation possibilities in regard to the understood principles.

4.7 KEY MANAGEMENT

If the issuer components decides to sign the credential data locally by itself (rather than using a remote signature service) it is important that the key management for the signature process is considered. The provider will have to consider different strategies for signing and key management depending on if they want to issue EAAs or QEAAs. Note that this component is not focusing on key distribution management yet, that will be something we will investigate at a later stage in the pilot when interfacing towards the verifiable data registries.

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

4.8 DATA STORE

The simplest integration of an authentic source and an issuer is done directly between them where the authentic source contains all the needed attributes to create and issue credentials. When the issuer needs the attributes, they can then be fetched on demand directly from the authentic source. This type of integration is however not always possible. Sometimes the authentic source infrastructure security classification does not allow that system to communicate with other systems except in very controlled environments. To enable the issuer to get access to the attributes needed to create and issue credentials it will in some circumstances be needed to have a separate data store where the authentic source can upload information using specified security measures. This intermediate data store can then more freely be accessed by the issuer and will then contain the needed attribute information to create and issue credentials. Using the separate data store is a possible way to achieve connectivity between certain authentic sources with legacy systems and very strict security policies and the wallet ecosystem at large in the pilots. It is however not the recommended approach, in the long run a direct connection between the authentic source and the issuer is recommended. The important point in this case is that it is up to the authentic source to choose how this should be implemented and the architecture should be modular enough to support different use cases. Using a data store is only one example how this could solve certain issues an authentic source has.

4.9 AUDITING

To be able to troubleshoot problems with the issuer and to be able to ensure that all the processes handled by the issuer have been done correctly there need to be auditing logs with relevant information. The extent of data stored by these logs will be investigated during the pilot. Storing data such as this is usually a balance between transparency and personal integrity of the individuals using the system and the functionality, maintainability and traceability of the system.

4.10 OPENID PROTOCOL ENGINE

The OpenID protocol engine will act as a frontend in the issuer and verifier towards the wallet ecosystem to enable the issuer and verifier to communicate using the OpenID standards. This component will e.g. implement the OpenID4VCI standard to issue credentials and OpenID4VP to verify the presentation of credentials. The OpenID protocol engine can also be used to handle authentication and authorization for the different use cases if that is needed.

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. RELYING PARTY

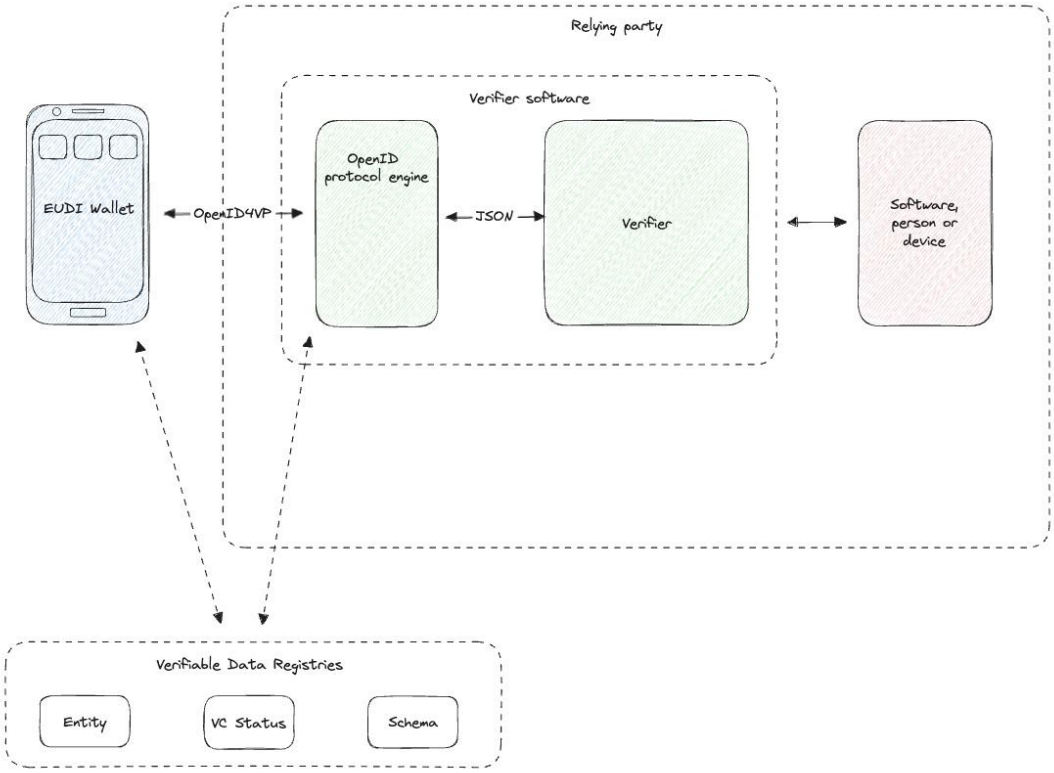

Figure 5: Relying party architecture suggestion

5.1 SOFTWARE, PERSON, DEVICE

The relying party will in many cases be either some kind of software verifying a credential (e.g. a diploma being verified by a university online), a person verifying a credential out in the field (e.g. an inspector verifying a PDA1 credential at a construction site) or a physical device (e.g. a NFC terminal verifying a EHIC at a doctor's office).

All of these cases will need help to interact with the new standards that are going to be used in the wallet ecosystem according to the ARF. In DC4EU WP7 we will build an open source verifier software that can be that intermediary solution to enable relying parties to interact and verify credentials in the wallet ecosystem.

5.2 VERIFIER

The verifier is the part of the software that primarily helps the relying party to understand the content of the credential attributes presented by the EUDIW and that contents validity.

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

5.3 OPENID PROTOCOL ENGINE

The OpenID protocol engine will act as a frontend in the issuer and verifier towards the wallet ecosystem to enable the issuer and verifier to communicate using the OpenID standards. This component will e.g. implement the OpenID4VCI standard to issue credentials and OpenID4VP to verify the presentation of credentials. The OpenID protocol engine can also be used to handle authentication and authorization for the different use cases if that is needed.

The engine will also look into adding support for SIOPv2.

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. REGISTRIES

For the wallet ecosystem to work there needs to be a governance in place that creates trust between the different entities that participate in this ecosystem. Both providers of credentials, wallet holders and relying parties need to be able to trust each others when issuing and verifying credentials.

The verifiable data registries will be part of the trust infrastructure creating that trust and it will be part of the pilots to ensure that this trust can be established and relied upon. One such solution is using EBSI. In DC4EU we see that the verifiable data registries are made up of a couple of different registries.

- One or more registries to create trust between the different entities participating in the ecosystem, e.g. issuers, verifiers and wallet solutions.
- A schema registry to ensure that both issuers, verifiers and the EUDI wallet can rely on the same understanding of credentials that are issued and verified.
- A registry or similar service that helps keep track of and distribute information about the status of credentials.

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. SUMMARY

The goal of this document is not to define the final architecture of the components that will be built in the DC4EU large scale pilot. The goal is to establish an overview of how an architecture for the issuer and verifier software can be visualized and to have a foundation to start the dialogue around the architecture that will be needed going forward.

Work package 7 in DC4EU will focus on building open source issuer and verifier components to help attestation providers and relying parties to integrate and interact with the EUDIW ecosystem.

The final revision of the eIDAS regulation and future changes in the ARF will be important topics to follow to ensure that the architecture of the components built in DC4EU follow those changes and are able to help achieve an interoperable EUDIW ecosystem.

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. REFERENCES

[1] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

[2] https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

[3] https://docs.google.com/spreadsheets/d/1Z4cYfjbbE-rABcfC-xab8miocKLomivYMUFibOh9BVo/edit#gid=1590639334

[4] https://openwallet-foundation.github.io/credential-format-comparison-sig/#/

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

ANNEX I – CREDENTIAL PROFILES

Verifiable credentials with SD-JWT-VC as base standard

- Aligned to W3C-VC
  - No
- Credential Format
  - SD-JWT-VC
- Signing Algorithm
  - ECDSA
- e-seals/e-signatures
  - PAdES and JWS
- jADES compliant
  - Pending to prove compliance
- Revocation Algorithm
  - Status List 2021
- Key Management (Issuer)
  - raw public keys (none jwk)
- Key Management (Holder)
  - did:jwk
- Trust Management
  - X.509 certificates

Verifiable credentials with “EBSI profile”

- Aligned to W3C-VC
  - Yes
- Credential Format
  - JSON-based VCs compatible with SD-JWT + SD-JWS
- Signing Algorithm
  - ECDSA
- e-seals/e-signatures
  - **jAdES** and JWS
- jADES compliant
  - Prove, tested, in use
- Revocation Algorithm
  - Status List 2021 + others
- Key Management (Issuer)
  - did:ebsi method 1 for legal entities
- Key Management (Holder)
  - did:ebsi method 2, simple public-key based DID method, for Natural Persons
- Trust Management
  - Decentralized PKI (also supports X.509v3)
  - EBSI Trust Lists (over Trust Registries)

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