Call for tender for the implementation of a personal identity wallet conformant to EU standards

TABLE OF CONTENTS

1 Introduction

Personal digital identity is perceived as a fundamental building block of the emerging digital market. We are all used to "informal" digital identities ("authenticate with Google", etc.), but this is insufficient for those contexts where full legal value is required (e.g., for access to health services, university services, banking services…). In many cases, ad-hoc authentication systems have been put in place (like UniPD SingleSignOn, or your own online bank authentication system), but they are limited to specific services and do not scale.

To address this issue, **national digital identity systems** have been created (in Italy: SPID, Carta di Identità Elettronica). In the EU, there is now an ongoing initiative aimed at providing EU citizens with an interoperable digital identity to be used across public and private digital services from different countries [1]. A recent regulation has been issued to this effect [2].

The EU regulation will find its way to the implementation through the obligation for EU Member States to implement and release a "digital identity wallet" which conforms to a set of standards, so that it can be used with any compliant service in any EU country.

The reference architecture for the EU digital identity wallet is presented in [3].

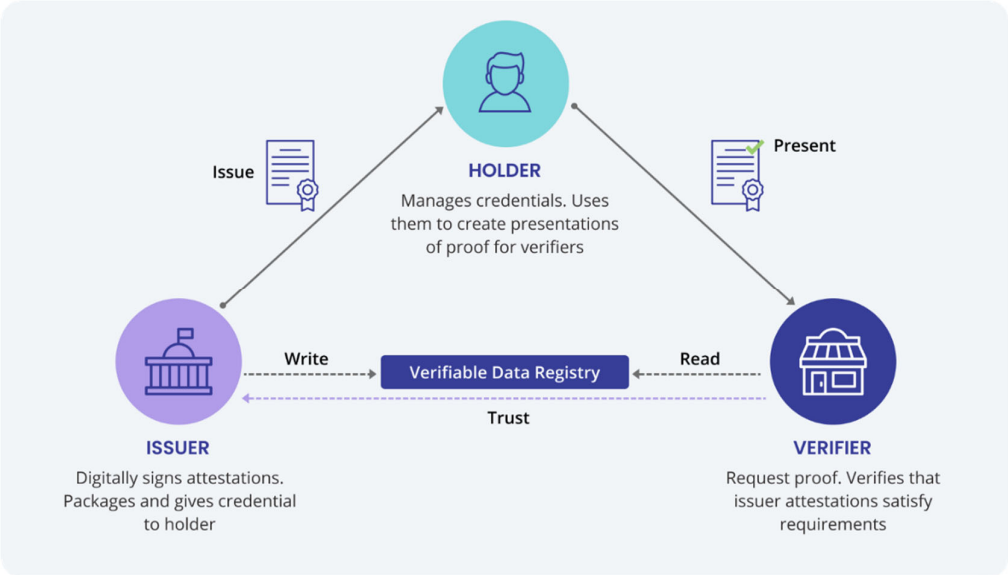
2 Reference model

The general idea is rooted around the concept of "verifiable credential". A verifiable credential is a file (usually, JSON) which contains some information about a subject, and which is signed (with digital signature) by the entity which takes the responsibility of claiming that information.

An example of a verifiable credential, issued by Infocert, which claims that the holder of the credential is "Alice Bobman", has fiscal code "LCABMB…", was born in Milan, etc.
(signature details omitted intentionally).

This is a second verifiable credential issued by UniPD, claiming that Alice has a degree in Electronic Engineering, etc.

The model has three main actors:



Issuer: institutions that issue credentials to Holders (e.g., UniPD issuing a university registration credential to you)
Holder: users who collect credential from different sources and store them in their identity wallet. The identity wallet may be a hosted service or an application run in a user device. The concept is analogous to crypto-wallets, which may be hosted (e.g. coinbase.com) or local (e.g. metamask.io, electrum.org). *For this project, we require a hosted wallet accessible via web.*
Verifier: entities interested in consuming credentials (e.g., an online bank asking for your university registration credential in order to offer you a student account). Credentials provided to a verifier by a holder may be packaged in "verifiable presentations"
Verifiable Data Registry: infrastructure that enables the verifier to validate the received information.

A user (Holder) will collect multiple credentials from several issuers into his/her wallet, and will use them multiple times toward several verifiers, according to the requested information. Note that *the wallet is a personal service for the user*, independent from any issuer/verifier. In many cases, the same entity may play several roles: UniPD may be an issuer of degree credentials but also a verifier of identity credentials.

3 PRODUCT REQUIREMENTS

3.1 Functional requirements

This is a list of high-level requirements. They will be refined in the course of the project.

N.	Title	Description	Notes
Credential issuing			
CI-1	Request a credential	A user (holder) must be able to navigate the issuer website and request a credential for his/her wallet	Issuer website will be a demo site, e.g., demouniversity.it
CI-2	Provide a credential	A back-office user (issuer side) must be able to issue a credential to a holder	
CI-3	Get a credential	A user (holder) must be able to get a credential from the issuer website	
Credential management			
CM-1	See credentials	A user (holder) must be able to see the set of received credentials via the web app	Note that the EU specification [3] describes a *mobile app*. This project work requires a *hosted wallet accessible via web*.
CM-2	Delete credential	A user (holder) must be able to remove a credential from the web app	
Credential consuming			
CS-1	Request credential (presentation)	A verifier must be capable to ask a user navigating its website to provide a credential (presentation) which is stored in the user's wallet	Verifier website will be a demo site, e.g. demoemployer.
CS-2	Provide credential (presentation)	A user (holder) must be able to provide to a verifier the credential (presentation) which has been asked for	

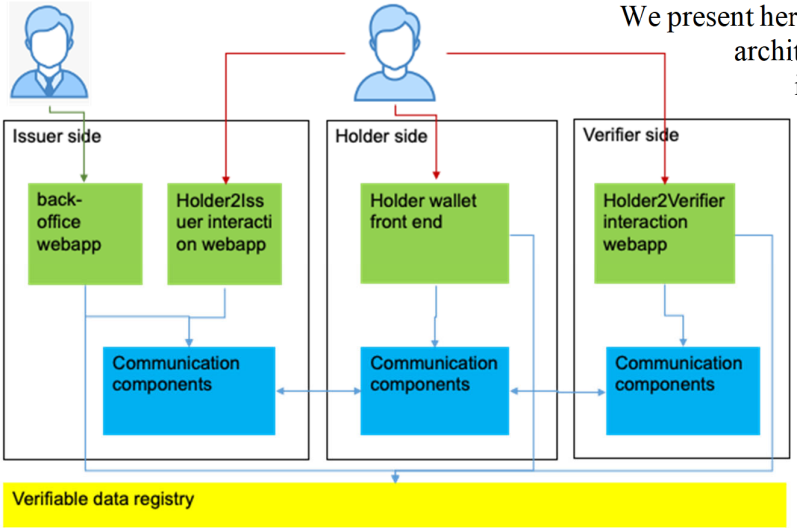
CS-3 (optional)	Credential validation	A verifier must be able to validate the correctness of the credential (presentation) received	

3.2 Non-functional requirements

N.	Title	Description	Notes
interoperability			
IO-1	Credential format	Credentials must respect the format JSON W3C	This is a subset of the options offered in [3]
IO-2	Protocol issuer-holder	Credentials must be exchanged using the protocol OpenID4VC	
IO-3	Protocol holder-verifier	Credentials must be exchanged using the protocol OpenID4VP	
usability			
US-1	User app friendliness	A user (holder) must feel confident about the operations he is performing on the walelt	
security			
SE-1	Credentials ownership	Credentials can only be spent by the effective holder	
SE-2	Credential untamperability	Credentials cannot be forged nor modified	
SE-2	Exchange confidentiality	Credentials cannot be eavesdropped during communication	

According to the EU timeline, there will be some reference implementations by Q1 2023. In case of delay, Infocert may provide reference components.

4 Reference architecture



We present here a downsized version of the architecture shown in [3], which is a suitable reference for the implementation of the prototype required in this project.

The necessary architectural components include:

- A **back-office component** (web app) to enable the issuer (an employee of the issuer organization) to manually check the request for credentials and authorize the issuing
- A **demo user interaction component** (web app) to enable the user (holder) to navigate and request specific credentials from an issuer (e.g., demouniversity site)
- A **demo user interaction component** (web app) to enable the user (holder) to navigate a verifier site and provide credentials as requested (e.g., demoemployer site)
- A **user front-end app** for the user to store and manage their credentials – a web app. Depending on time and resources this may be a mobile application or a browser plug-in.
- A **communication component** to enable the exchange of credentials/presentations according to a standard protocol – the communication component will be deployed three times in the three contexts (issuer side, holder side, verifier side)

A **verifiable data registry** which offers services to validate credentials will not be required for this project – we assume that credentials will be always valid.

From an implementation perspective, there is no restriction on whether to implement a single web app/PWA[1] which supports all functionalities (and which is deployed several times), or separate apps for each set of functionalities. The communication component can be implemented as a library or as an active component (an "agent").

It is recommended to use open-source code made available by the community, whenever possible.

[1] Progressive Web App: https://web.dev/progressive-web-apps/

A sample front end will be made available by Infocert as a guiding example or as a starting point for implementation.

4.1 Expected deliverable items

The following deliverable items are expected of this project:

- Descriptive document and deployment instructions (user manual)
- Software components (GitHub)
  - User/installation manual
  - Design documents
  - Code
  - Test suites and test results
- Deployment in a local setting.

5 INFOCERT UNDERTAKINGS

During the project execution, Infocert will provide support in the following ways:

- Bi-weekly progress reviews (as a product owner)
- Provision of building blocks (open-source libraries, etc.)
- Availability of expert personnel for helping with blocking challenges.

REFERENCES

[1] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
[2] https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation
[3] https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

Contatti proponente

- Luca Boldrin <luca.boldrin@unipd.it>
- Alessandro Visintin <alessandro.visintin@infocert.it>
- Gianluca Markos <gianluca.markos@infocert.it>
- Davide Porro <davide.porro@infocert.it>