Deliverable 2.1

Requirements Document

Verein zur Förderung der selbstständigen Nutzung von Daten
2540 Bad Vöslau
ZVR: 789007092

Contact: office@ownyourdata.eu

Content

1 Introduction

This deliverable describes the requirements in the FFG funded IDunion project.

The document includes a general introduction to the project, the methodology including a stakeholder analysis, and the actual requirements. The document is concluded with an outlook and a glossary.

1.1 Background

Currently, vaccination and immunisation information are spread over different organisations like labs and hospitals as well as pharmaceutical companies together with government agencies. A patient usually only has a paper certificate that provides vaccination treatments with often difficult to read handwritten additional information. Recently, the COVID-19 pandemic led to new momentum in digital health passes and many citizens now use an app on their smartphone to store and present vaccination and test credentials.

The main focus of this project is on data interoperability and self-sovereign management of vaccination information. Additionally, it addresses data transparency (through usage policies and provenance information) and security & privacy issues (by applying blockchain technology and digital watermarking on data sharing).

1.2 Relation to other deliverables

This requirements document is one out of two documents providing the detailed description about this project:

- D2.1 Requirements Document: lists functional and non-functional requirements for creating and verifying credentials, as well as sharing data between individuals and organisations
- D2.2 Design Specification: describes and depicts the system design together with API endpoints and data formats of the various components

2 Methodology

This section presents the performed work in the project regarding requirements elicitation, current status, and outlook for further development.

In the course of the project the following steps were performed:

- Identify relevant list of stakeholders and describe their needs as well as their environment where they operate and make decisions
- Describe requirements (this document) and deduce the Design Specification (D2.2)
- Setup a dedicated test system for deploying and verifying available components and iteratively feedback any learnings
- Deploy solution with partners and collect further feedback

2.1 Stakeholders

Initially, a list of relevant stakeholders was compiled:

- Individual with a mobile wallet installed on smartphone
  (tag: wallet)
- Individual with interest in self-monitoring who has a personal data store (PDS) account
  (tag: user)
- Clinician performing the process of vaccination and issuing a verifiable credential
  (tag: clinician)
- Officer verifying the health status at a checkpoint, e.g., airport
  (tag: officer)
- Organisation performing studies and seeking data from individuals
  (tag: org)
- Government & politics for establishing legal circumstances for health documents
  (tag: gov)
- Verifiable data registry acting as a trust anchor for identity information, in this project the IDunion SSI network
  (tag: dlt)
- Data intermediary providing means for individuals to collect, store, and process personal data, e.g., MyData-Operators
  (tag: operator)

All requirements were mapped to at least one of those stakeholders to document source and motivation. During the course of the project a data flow will be implemented that demonstrates creating and verifying a COVID-19 credential for an individual as well as exchanging personal health data between an individual and an organisation.

2.2 Standards

In the course of the project the following standards were identified and are adhered to in developing the system:

- **Decentralised Identifier (DIDs)** for managing identities of end-users;
  described in detail here: https://www.w3.org/TR/did-core/
- **Verifiable Credentials** data model;
  described in detail here: https://www.w3.org/TR/vc-data-model/
- **Data Privacy Vocabulary** for consent management;
  described in detail here: https://w3c.github.io/dpv/
- **Vaccination Status** - Digital Documentation of COVID-19 Certificates
  described in detail here: https://github.com/WorldHealthOrganization/ddcc
  - also use Vaccination Certificate Vocabulary:
    https://w3c-ccg.github.io/vaccination-vocab/
- **Representation of medical data** follows FHIR where applicable;
  - Communication - https://www.hl7.org/fhir/communication.html
  - Patient - https://www.hl7.org/fhir/patient.html
  - RelatedPerson - https://www.hl7.org/fhir/relatedperson.html
  - Immunisation - https://www.hl7.org/fhir/immunization.html
  - Organisation - https://www.hl7.org/fhir/organization.html

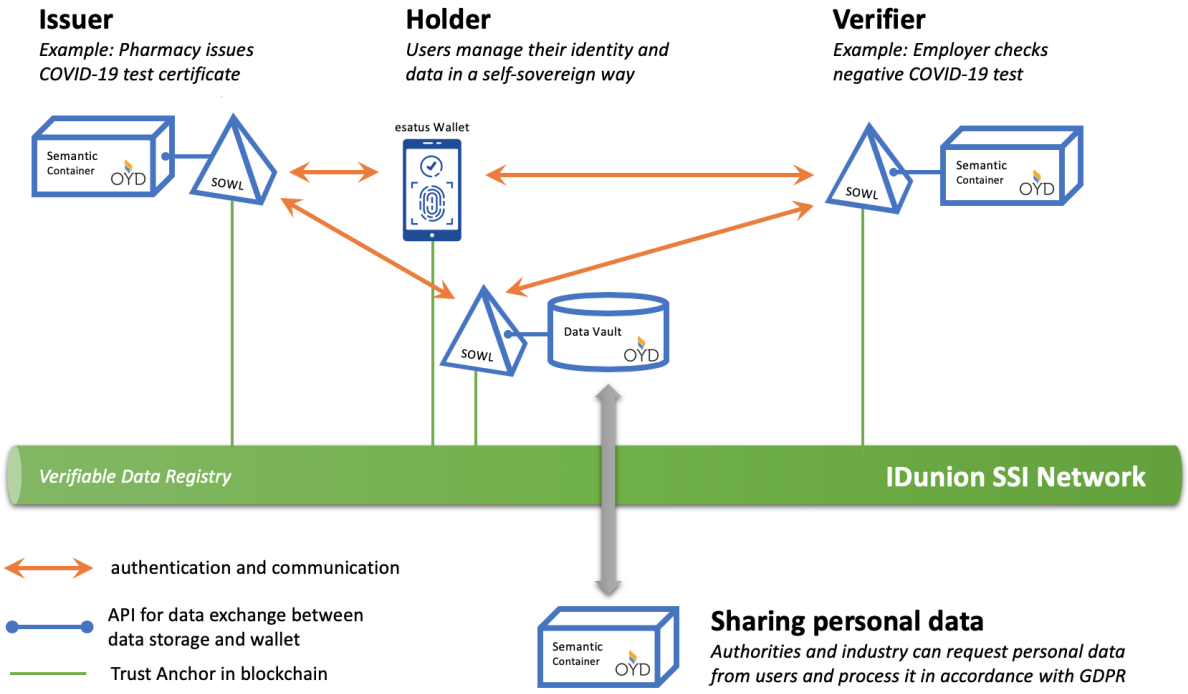
2.3 Maintenance and next steps

Initially the Digital Immunisation Passport project (funded by NGI DAPSI) and now its successor project in collaboration with IDunion funded by FFG sparked interest from multiple organisations and industry partners. We continue to collaborate with those companies and initiatives to provide valuable input in developing the new standards for human-centric and self-sovereign digital health passports.

3 Requirements

3.1 Overall description

Human-centric health data and especially immunisation information management faces a number of challenges, some of which we are addressing in this project. Typically, data sets provided by health institutions differ greatly in format and content. We will be utilising Semantic Overlay Architecture (SOyA), a flexible multi-dimensional schema architecture, to facilitate a unified data language so that harmonised data can be held in Semantic Containers and made accessible to Personal Data Stores. We will use the IDunion SSI network as a government-based trust anchor for identities of individuals/institutions to prove vaccination and test certificates, while using self-issued decentralised identifiers for sharing personal data. Every data exchanged requires consent using machine-readable and automatically processed usage policies. A full provenance trail documents data exchange including consent and validation results.



3.2 Building blocks

3.2.1 Semantic Container

Semantic Containers provide a standardised infrastructure for data provisioning and allow data providers to efficiently distribute data without giving up control over its usage and monetization while providing data consumers with efficient and well-managed mechanisms to obtain and integrate data in a trustworthy and reproducible manner. By packaging data and processing capabilities into reusable containers, describing the semantics of the content and permissible usage, and providing uniform interfaces, a data set becomes a commodity with well-defined content, properties, quality, and usage policy, as well as clear ownership rights and a price tag.

The Semantic Container approach leverages existing container technologies such as Docker, which already provide scalable mechanisms for deploying complex software assemblies and use them as a foundation for an infrastructure for data discovery, provisioning, and integration. To create a suitable environment for the emergence of a commodity market around data, a set of rules for permissible usage of the data is captured in semantic descriptions, provides cryptographic methods to prove ownership rights, and applies blockchain technology to guarantee immutability. Complete audit trails of data sources and processing steps provide gapless provenance and facilitate reproducibility.

3.2.2 Personal Data Store

The OwnYourData Data Vault is a Personal Data Store based on the following principles:

- Open & Free: all code is available under the MIT open source licence on Github and the service is hosted for free under https://data-vault.eu
- Secure: personal data is stored encrypted (asymmetric encryption allows plugins to write data using a public key) and data processing services are executed in a restricted environment ("sandbox") to ensure information is not leaked externally
- No lock-in: choose where you want to store and process your data / move data and services to your trusted location
- Extensible: plugins allow to add any 3rd party services (data sources, data processing services, and visualisation methods) with fine-granular permission settings
- Audited: to guarantee immutability and timeliness of all operations (login, plugin changes, data operations) a linked audit log is maintained and hash values are stored in the Ethereum blockchain
- Standard compliant: where applicable available standards are used (authentication, data formats, API endpoints) and through active collaboration in various groups and organisations additional standards will be adopted

In this project the OwnYourData Data Vault provides the human-centric personal data management that interfaces to Semantic Containers and the SOWL cloud wallet.

3.2.3 Wallet

This project uses the commercial cloud wallet SOWL provided by esatus AG:
https://esatus.com/solutions/self-sovereign-identity/sowl/

3.2.4 Distributed Ledger

This project uses the German IDunion SSI network described here: https://idunion.org/

3.3 Non-functional requirements

3.3.1 Performance and scalability

Requirements that describe throughput under a given workload for a specific time frame in each setting.

ID	Tags	Description
perf_1	operator, user	The personal data store shall handle at least 100.000 registered users.
perf_2	clinician, officer	A Semantic Container shall handle at least 10.000 user interactions.

3.3.2 Portability, compatibility, and interoperability

Requirements to make sure that the system can be operated now and in the foreseeable future on the available platform infrastructure and also works together with adjacent systems.

ID	Tags	Description
port_1	wallet, user, org, gov, operator	Available standards and best practices for the respective areas should be identified and adhered to.
port_2	org, gov, operator	Data exchange between building blocks shall use JSON.
port_3	gov, operator	The interfaces of the different components shall be clearly defined and documented.
port_4	gov, operator	Data structures shared between components shall follow a publicly available schema (in this project using Semantic Overlay Architecture).

3.3.3 Reliability, availability, and maintainability

Requirements describing the accessibility of the system to the users at a given point in time and how to quickly recover from any failures.

ID	Tags	Description
rel_1	user, clinician, officer, operator, org	Components shall be easy to deploy and configure (in this project using Docker containers).
rel_2	user, clinician, officer, operator, org	All software components shall be documented.
rel_3	user, clinician, officer, operator, org, gov	Essential information shall be stored in immutable and redundant form (e.g., in a distributed ledger).

rel_4	user, clinician, officer, org	The system shall perform input validation.

3.3.4 Privacy and security

Requirements about privacy (safeguarding data) and security (authorization and protection) needs from different stakeholders.

ID	Tags	Description
priv_1	user, org, gov, operator	All external data transfer shall be encrypted.
priv_2	user, operator	All vaccination and immunisation information stored in the PDS shall be encrypted.
priv_3	clinician, gov, dlt	The history of vaccination events shall be stored in a consistent and immutable form.
priv_4	user, clinician, officer, gov	Consent between data subject and data controller for data exchange (here especially health data) shall be visually indicated and inseparably linked to the payload.

3.3.5 Localization

Specify requirements in line with the context of the target audience.

ID	Tags	Description
loc_1	user, clinician, officer, org	The user interface shall support multiple languages.
loc_2	user, clinician, officer, org	The user interface shall be available at least in English and German.

3.3.6 Usability

Requirements that define the ease-of-use for the system.

ID	Tags	Description
usab_1	wallet, user	The user interface for end-users shall be usable on a mobile phone screen (in this project responsive design will be used).

3.4 Functional requirements

3.4.1 Onboarding of stakeholder

This section describes the functional requirements to ensure stakeholders have a digital identifier and the necessary components installed in their respective systems.

ID	Tags	Description
onb_1	wallet	An individual shall be able to create an account to use a digital wallet for managing verifiable credentials on a smartphone. Android and iOS shall be supported by the digital wallet.
onb_2	user	An individual shall be able to create an account in a PDS.
onb_3	wallet, user	An individual shall be able to pair the account for digital wallet and PDS. It shall be possible to use the identity from the digital wallet to login into the PDS.
onb_4	clinician, gov, dlt	A clinician shall have the infrastructure to issue verifiable credentials for vaccinated users.
onb_5	clinician, user, dlt, operator	Legal entities (clinician, officers) shall be able to share / read issued verifiable credentials with the wallet and/or PDS of a user.
onb_6	clinician, user, gov	Legal entities (clinician, officers, organisations) shall be able to specify a Usage Policy to describe how user data is handled.
onb_7	user, gov	A user shall be able to specify preferences in the form of a Usage Policy and the system shall automatically report compliance or deviations upon data exchange with 3rd parties.
onb_8	gov, org	An organisation that performs data sharing or collecting activities shall provide infrastructure to manage jurisdictional compliant data processing.

3.4.2 Creating verifiable credential

This section describes functional requirements for the "Create Verifiable Credential" data flow. Requirements in this section define gathering information on the user side, requesting and storing the credential.

ID	Tags	Description
cre_1	wallet, user, clinician	An individual shall be able to scan a QR code from a clinician to retrieve and verify the following information: - type of credential that can be provided, - information about the clinician, - information about the vaccine to be received, - Usage Policy how data provided from the user is handled.

cre_2	wallet, user, clinician	An individual shall be able to request vaccination by providing the relevant personal data and consenting to the clinicians Usage Policy.
cre_3	user	A user with a PDS account shall be able to store personal information required for requesting a verifiable credential for vaccination.
cre_4	user, clinician	A clinician shall be able to receive a request for vaccination from a user.
cre_5	clinician, dlt	A clinician shall be able to issue a verifiable credential related to the vaccine given to a user.
cre_6	clinician	A clinician shall be able to store information related to the vaccine event.
cre_7	wallet, clinician	An individual shall be able to receive the verifiable credential from the clinician.
cre_8	user, clinician	A user shall be able to store information of the received verifiable credential in a PDS.
cre_9	user	A user shall be able to list all verifiable credentials in the PDS and show for each element at a minimum the following attributes: type, issuer, validity duration, creation date.

3.4.3 Verifying a credential

This section describes functional requirements for the "Verify Credential" data flow. The section focuses on managing and presenting the credentials created during the vaccination process.

ID	Tags	Description
ver_1	user	A user shall be able to scan a QR code from a checkpoint to retrieve and verify the following information: - information about the officer and the organisation/government he/she acts on behalf, - type of credential that will be verified, - Usage Policy how data provided from the user is handled by the checkpoint.
ver_2	user, officer	A user shall be able to send the following information based on a verification request: - one or more verifiable presentations, - confirmation to the presented Usage Policy from the officer.
ver_3	officer	An officer shall be able to identify itself and the organisation to which they belong.
ver_4	wallet, user	A user shall be able to prove control over the verifiable credential.

ver_5	officer	An officer shall be able to receive a verifiable presentation from an individual.
ver_6	officer	An officer shall be able to store the results of the verification (passed/not passed) together with other metadata according to the presented Usage Policy.
ver_7	officer, wallet, user	An offer shall pass the information about successful / unsuccessful verification along to the respective user.
ver_8	user	A PDS shall document any verifier and verification result of a verifiable presentation.
ver_9	user	A user shall be able to access and review all information linked to a verifiable credential. (Especially, users shall be able to access revocation information required for understanding the reason for rejection.)

3.4.4 Sharing data

Requirements in this section define the complete process of data sharing from contacting participants, selecting and submitting a data set, as well as tracing shared data.

ID	Tags	Description
sha_1	org, gov	An institution requesting data from users shall provide at least the following information: - information about the institution and purpose of the data sharing request, - a service endpoint where data should be sent to, and - a Usage Policy describing how data provided by the user is handled by the institution.
sha_2	org	A data sharing request shall be sent via email to users with a personalised invitation token.
sha_3	operator	The PDS shall support processing the invitation token to collect and present the user with all necessary information from the institution requesting the data.
sha_4	user	A user shall be able to select what data should be shared with an organisation for a concrete data sharing invitation.
sha_5	operator	The PDS shall store information about sending data in the course of data sharing - this includes: - information about the institution and purpose of the data sharing request, - the service endpoint where data is sent to, - the Usage Policy describing how data provided by the user is handled by the institution, - survey data and list of records that are shared.

sha_6	operator	The PDS shall provide means to manage digital watermarking for time series data when sharing data. Note: this includes handling dataset fragments, providing identical watermarking for same requests, and identifying the receiver of a suspicious dataset
sha_7	org, user	An institution that invites users to share data shall provide confirmation upon receiving data from a user.
sha_8	org, gov, user	An institution that has received personal data shall allow users to query when this data was accessed and is required to document conformance to the initially published usage policies.
sha_9	org, gov, user	An institution that has received data shall allow users to later revoke consent for provided data.

4 Conclusions

This document outlined the requirements identified in the initial design phase of the IDunion project. Based on a stakeholder analysis and the goals defined in the project proposal the main components where identified and non-functional as well as functional requirements were documented. Based on these requirements the design is described in deliverable D2.2 Design Specification.

Appendix

Glossary

Below is a list of acronyms and abbreviations used throughout the document.

Acronym	Description
DID	Decentralised Identifier
PDS	Personal Data Store (in this project: OwnYourData Data Vault)
VC	Verifiable Credential
SPECIAL	Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance (project website: https://www.specialprivacy.eu/)