Horizon 2020 Programme
DG CNECT
Next-generation Internet

Project acronym: **DIP**

Project title: **Digital Immunization Passport**

Deliverable 2.1

Requirements Specification

Deliverables leader:	**OwnYourData**
Authors:	Christoph Fabianek, Eduard Gringinger, Gabriel Unterholzer, Philippe Page, Paul Knowles, Robert Mitwicki, Meri Seistola
Due date:	2020-11-20
Actual submission date:	2020-11-20
Dissemination level:	Public

Abstract: This report is part of a third-party project DIP that has received funding from the NGI_DAPSI (DAPSI open call), the European Union's Horizon 2020 research and innovation programme under grant agreement No. 871498.

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

Document Revision History

Date	Version	Author/Editor/Contributor	Summary of main changes / Status
2020-09-07	0.1	Christoph Fabianek	Initial document
2020-11-20	1.0	Christoph Fabianek	First public version
2021-01-21	1.1	Christoph Fabianek	updates towards 2nd evaluation
2021-05-31	1.2	Christoph Fabianek	final updates at project end

Disclaimer

Copyright

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

Table of content

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

Executive Summary

The deliverable describes the requirements in the Digital Immunization Passport (DIP) project.

The document includes a general introduction to the project in chapter 1, the methodology including a stakeholder analysis in chapter 2, and the actual requirements in chapter 3. The document is concluded with an outlook and a glossary.

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

1 Introduction

1.1 Background

Currently, vaccination and immunization information are spread over different organizations 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.

The main focus of this project is on Data Interoperability & Compatibility through establishing interfaces between health industry and individuals as well as pushing forward on standardized interfaces for PDSs. Additionally, we address Data Transparency (Usage Policies and Data Provenance in Semantic Containers) and Security & Privacy (by applying blockchain technology and digital watermarking on data sharing).

1.2 Relation to other DIP 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 organizations
- D2.2 Design Specification: describes and depicts the system design together with API endpoints and data formats of the various components

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

2 Work done and current status

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

2.1 Methodology

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

2.2 Results and discussion

2.2.1 Stakeholders

Initially, a list of relevant stakeholders was compiled:

- Individual with a personal data store (PDS) account
  (tag: user)
- Clinician performing the process of vaccination or assessing the immunization status and issuing a verifiable credential
  (tag: issuer)
- Hospitals, laboratories, and doctors offices employing clinicians and providing the administrative infrastructure
  (tag: lab)
- Officer verifying the health status at a checkpoint, e.g., airport
  (tag: verifier)
- Identity provider using e.g. biometric features, government issued documents. or other intelligence as basis for a reproducible identifiers of individuals or organizations
  (tag: idp)
- Organization performing studies and seeking data from individuals
  (tag: org)
- Government & politics for establishing legal circumstances for health documents
  (tag: gov)
- Data Store Operators: providing means for individuals to collect, store, and process personal data, e.g., MyData-Operators
  (tag: pds)

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

All requirements were mapped to at least one of those stakeholders to document source and motivation. Additional feedback from the respective groups is added in each section when new input becomes available.

During Phase 1 of the DIP project simple use cases with the stakeholders listed above will be implemented and presented in a tech-demo. In Phase 2 more complex workflows will be developed based on the available framework and providing production-ready real-life scenarios. Requirements that will be implemented in this second phase are tagged "phase2".

2.2.2 Standard

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

- Decentralized 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/
- Representation of medical data follows FHIR where applicable;
  FHIR profiles for Immunizations submissions are derived from a number of resources (see Figure 2.1), including:
  - Communication - https://www.hl7.org/fhir/communication.html
  - Patient - https://www.hl7.org/fhir/patient.html
  - RelatedPerson - https://www.hl7.org/fhir/relatedperson.html
  - Immunization - https://www.hl7.org/fhir/immunization.html
  - Organization - https://www.hl7.org/fhir/organization.html

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

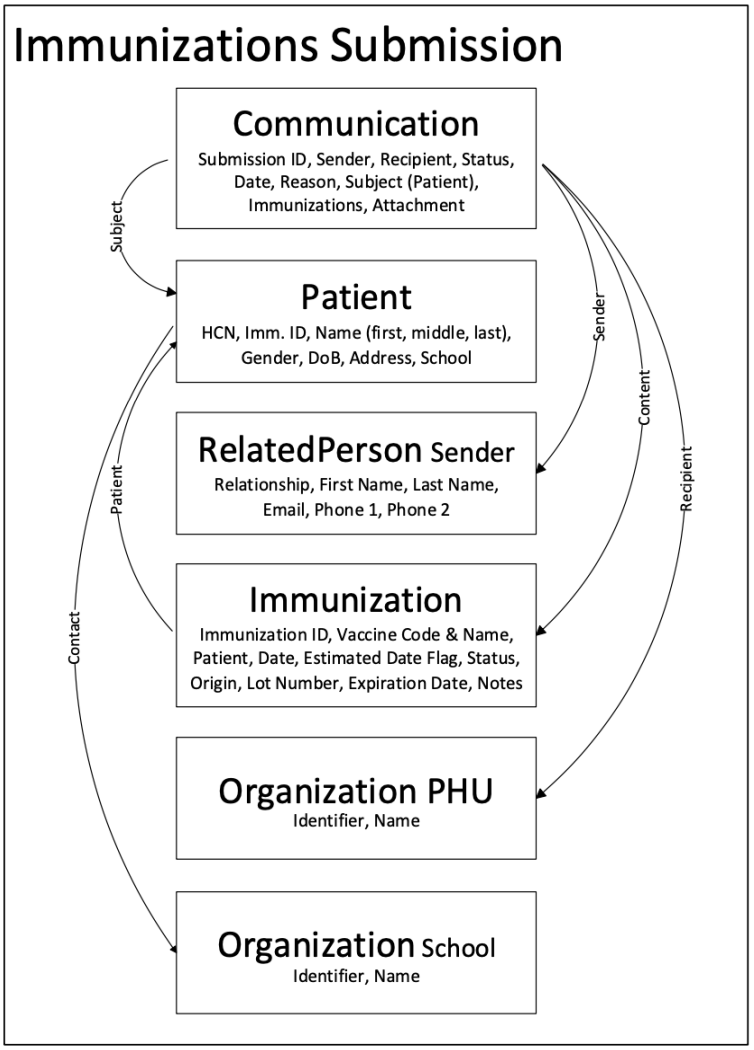

Figure 2.1: FHIR Immunization Submission

2.3 Maintenance and next steps

The Digital Immunization Passport project sparked a lot of interest from the very beginning and multiple organization and industry partners already supported the initial proposal: CANImmunize (Canadian digital immunization platform), iRespond (providing privacy protected digital identityI, MyData Global (empower individuals by improving their right to self-determination regarding their personal data), Novartis (Swiss multinational pharmaceutical company), and Personium (an open source decentralized Personal Data Store). We continue to collaborate with these companies and initiatives and also already successfully reached out to government officials to provide input on human-centric health data management especially in regard to the new European Data Strategy.

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

3 Requirement Specification

3.1 Overall Description

Human-centric health data and especially immunization information management faces a number of challenges that we plan to address in this proposal. Typically, data sets provided by health institutions differ greatly in format and content. We will be utilizing Overlays Capture Architecture (OCA), 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 using Common Endpoints inspired interfaces for Personal data Stores (CEPS).

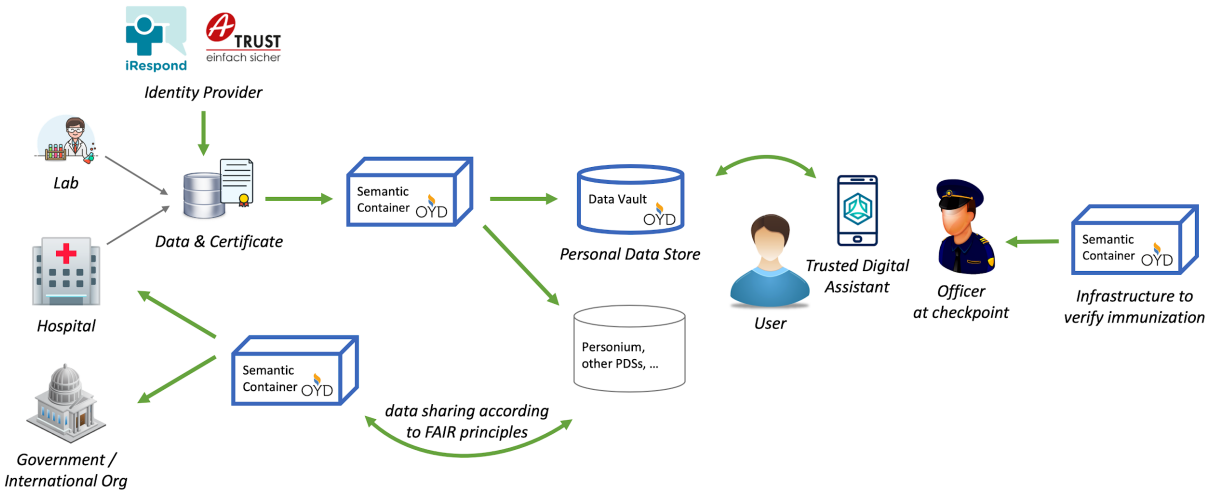

Figure 3.1: Overview

3.2 Building Blocks

3.2.1 Personal Data Store

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

- *Open & Free:* all code is available on Github under https://github.com/ownyourdata/oyd-pia2 and the service is available 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 visualization methods) with fine-granular permission settings

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

- *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 organizations additional standards will be adopted

In the DIP project the OwnYourData Data Vault provides the human-centric personal data management that interfaces to Semantic Containers and the Trusted Digital Assistant.

3.2.2 Overlays Capture Architecture

Overlays Capture Architecture[1] (OCA) is an architecture that presents a schema as an amalgamated object consisting of a *schema base* and *overlays*. Overlays are task-oriented linked data objects that provide additional extensions, coloration, and functionality to the schema base. This degree of object separation enables issuers to make custom edits to the overlays rather than to the schema base itself. In other words, multiple parties can interact with and contribute to the schema structure without having to change the schema base definition. With schema base definitions remaining stable and in their purest form, a common immutable base object is maintained throughout the capture process which enables data standardisation.

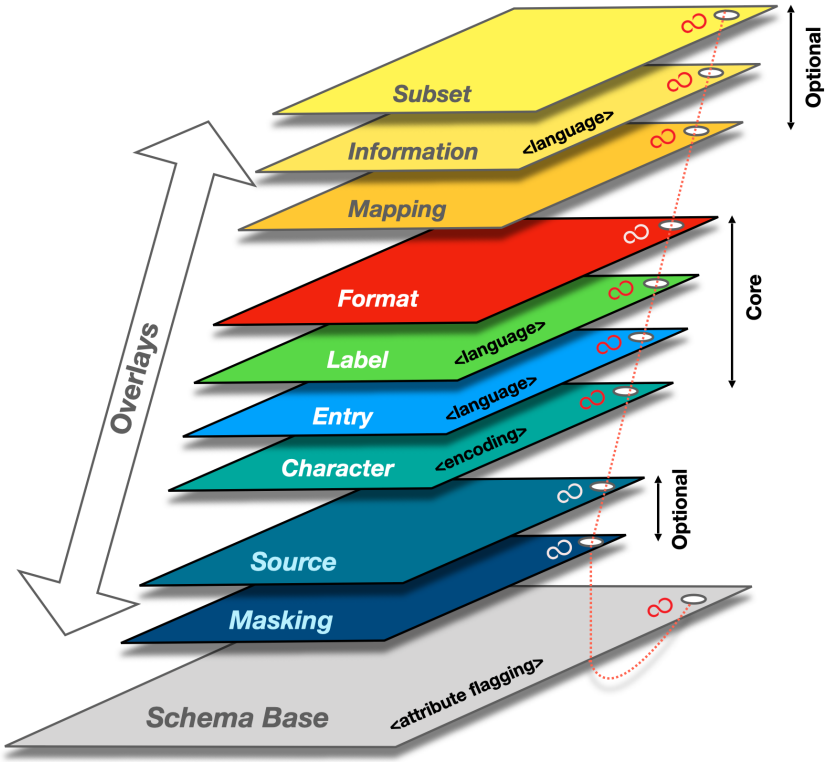

Figure 3.2: Overlays

[1] https://humancolossus.foundation/blog/cjzegoi58xgpfzwxyrqlroy48dihwz

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

All pre-standards work for OCA is being done in the Inputs and Semantics Working Group[2] at the Trust over IP Foundation[3].

3.2.3 Trusted Digital Assistant

A Trusted Digital Assistant (TDA) - based on the Hyperledger Aries toolbox[4] - is a user friendly interface for dynamic data economy. It allows the user to manage his/her identity, data with consent, allow for decentralized interaction with other entities and services. TDA is a set of applications running cross platform which helps users to manage digital assets.

A TDA enables users to exchange Verifiable Information, can proof claims and verify them.

References:

[1] The Current and Future State of Digital Wallets, Continuumloop Inc.:
https://gallery.mailchimp.com/31af1ca9b99d7761be02412c0/files/eab21be2-78ae-4eb8-a081-64de9d6059aa/The_Current_and_Future_State_of_Digital_Wallets_v1.0_FINAL.pdf

[2] Universal Wallet, Transmute, W3C Draft Specification:
https://transmute-industries.github.io/universal-wallet/

3.2.4 Semantic Container

Semantic Containers provide a standardized 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.

[2] https://wiki.trustoverip.org/display/HOME/Inputs+and+Semantics+Working+Group
[3] https://trustoverip.org
[4] https://github.com/hyperledger/aries-toolbox

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

3.2.5 Usage Policies

A Usage Policy is meant to express both the data subjects' consent and the data usage policies of data controllers in formal terms, understandable by a computer, so as to automatically verify that the usage of personal data complies with data subjects' consent. In other words it specifies a set of authorized operations within a Personal Data Store or a Semantic Container. Such authorized operations are characterized by:

- Data Categories: the data processed by the operation
- Purpose: the purpose of the operation
- Processing: a description of the operation itself
- Recipient: the entities that can access the result of the operation
- Storage: a description of
    - Location: where the result is stored and
    - Duration: for how long the data is allowed to be stored

Usage Policies were developed in the course of the EU funded SPECIAL project (https://www.specialprivacy.eu) and its further development is continued in the W3C DPVCG (https://www.w3.org/community/dpvcg/) - Data Privacy Vocabularies and Controls Community Group.

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	pds, user	The personal data store shall handle at least 100.000 registered users.
perf_2	issuer, gov	A Semantic Container shall handle at least 10.000 user interactions.
perf_3	lab, phase2	A lab shall handle at least 10 clinicians.

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.

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

ID	Tags	Description
port_1	gov, org	Available standards and best practices for the respective areas should be identified and adhered to.
port_2	org	Data exchange between building blocks shall use JSON.
port_3	pds	The PDS shall follow a public and fully documented API for accessing the data (e.g., being based on CEPS - common endpoints for personal data stores)
port_4	gov	Data structures shared between components shall follow a publicly available schema (in this project this is the Overlay Capture 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	lab, pds	Server components shall be made available as Docker containers.
rel_2	user	UI components shall use responsive design.

3.3.4 Security

Requirements about authorized access and protection.

ID	Tags	Description
sec_1	gov	All external data transfer shall be encrypted.
sec_2	pds	All vaccination and immunization information stored in the PDS shall be encrypted.

3.3.5 Localization

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

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

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

3.3.6 Usability

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

ID	Tags	Description
usab_1	user	Any user interface towards the user shall be usable on a mobile phone screen.

3.4 Functional Requirements

3.4.1 Onboarding of stakeholder

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

ID	Tags	Description
onb_1	user	A user should be able to access the OYD App (UI for PDS) and the TDA on their mobile device.
onb_2	user	The TDA shall manage a user's existing trusted digital identities.
onb_3	user	A user shall be able to create and manage a digital identity.
onb_4	user, gov, phase2	The system shall be able to handle biometric onboarding (not necessarily associated to / stored in a PDS).
onb_ 4.1	idp, phase2	The system shall allow to unambiguously link a string as identifier to an individual or an organization. *note: such a string can be either a GUID from an iris scan, a Legal Entity Identifier (LEI), or an eIDAS compatible signature of a document*
onb_ 4.2	lab, gov, phase2	The system shall support linking employees to organizations. *note: organizations and employees can in turn have unambiguous strings identifying them*
onb_5	issuer, lab	A lab shall provide the infrastructure for clinicians to issue verifiable credentials for vaccinated users.
onb_6	issuer	The TDA shall manage a clinician's existing trusted digital identity.
onb_7	lab, gov, org, phase2	Every organization shall be able to create and manage a GLEIF digital identifier.

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

onb_8	lab, issuer, phase 2	A lab shall be able to register and remove clinicians.
onb_9	lab	A lab shall import/export information about the vaccination process.
onb_10	lab, gov, org	Every organization shall be able to specify a Usage Policy to describe how user data is handled.
onb_11	user	A user shall be able to specify a Usage Policy to describe how his or her data is handled.
onb_12	verifier	A checkpoint shall provide infrastructure for officers to verify credentials from users.
onb_13	gov, org	Every organization that performs data sharing activities shall provide infrastructure to manage jurisdictional compliant data processing.

3.4.2 Create 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 managing the credential.

ID	Tags	Description
cre_1	user	A user shall be able to scan a QR code from a lab 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 in the lab.
cre_2	user, issuer, phase2	A lab shall be able to specify what immunization information is necessary prior to providing vaccination. This additional information request shall be included in the information provided through the QR code in requirement. cre_1. *note: for certain vaccines it is necessary to provide information about previously received immunizations, e.g., booster shots*
cre_3	user	A user shall be able to request treatment from a clinician by - sending a request for a defined verifiable credential, - providing the relevant personal information,

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

		- confirming the presented Usage Policy of the lab.
cre_4	user	A user shall be able to store personal information required for requesting a verifiable credential in a PDS.
cre_5	lab, issuer	A clinician shall be able to receive a request for treatment from a user.
cre_6	issuer	A clinician shall be able to select a request for treatment from a list of treatments.
cre_7	issuer	A clinician shall be able to issue a verifiable credential related to the vaccine given to a user.
cre_ 7.1	idp, phase2	A verifiable credential shall allow to include references to the issuing organization and/or employee in the payload.
cre_8	issuer, lab	A clinician shall be able to store information related to the vaccine event.
cre_9	user	A user shall be able to store information of the received verifiable credential in a PDS.
cre_10	user	A user shall be able to list all available verifiable credentials in the PDS.
cre_11	user	A user shall be able to show at a minimum the following attributes for each verifiable credential: type, issuer, validity duration, creation date, issued by.
cre_12	pds, lab	Any exchange between PDS and lab shall use DID Auth methods for authentication between user and clinician and DID Comm for secure and private communication between user and clinician.

3.4.3 Verify Credential

This section describes functional requirements for the "Verify Credential" data flow. The section focuses on 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 organization/government he/she acts on behalf, - type of credential that will be verified,

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

		- Usage Policy how data provided from the user is handled by the checkpoint.
ver_2	user	A user shall be able to send the following information based on a verification request: - one or more verifiable credentials, - confirmation to the presented Usage Policy from the checkpoint.
ver_3	verifier	An officer shall be able to identify itself and the organisation to which they belong.
ver_4	verifier, phase2	An officer shall be able to prove they are authorised and there is a legitimate purpose to request a vaccine credential.
ver_5	user	A user shall be able to prove control over the verifiable credential.
ver_6	verifier	An officer shall be able to receive a verifiable credential from a user.
ver_7	verifier	An officer shall be able to select a verifiable credential from a list of user submissions.
ver_8	verifier	An officer shall be able to store the results of the verification (passed/not passed).
ver_9	verifier	An offer shall pass the information about successful / unsuccessful verification along to the respective user.
ver_10	pds	A personal data store shall document any verifier and verification result of a verifiable credential.
ver_11	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.)
ver_12	pds, verifier	Any exchange between PDS and Verifier shall use DID Auth methods for authentication between user and officer and DID Comm for secure and private communication between user and officer.

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

3.4.4 Share Data

Requirements that 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, gov	A data sharing request shall be sent via email to users with a personalized invitation token.
sha_3	pds	The PDS shall support processing the invitation token to collect and present 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 organization.
sha_5	pds, user	The system shall support the user in automatically filling fields in surveys with existing data (e.g., first name, last name, gender).
sha_6	pds	A personal data store 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_7	pds	A personal data store shall provide all means to manage digital watermarking for time series data when sharing data. (This includes handling dataset fragments, providing identical watermarking for same requests, and identifying the receiver of a suspicious dataset.)
sha_8	org, gov	An institution that invites users to share data shall provide confirmation upon receiving data from a user.
sha_9	org, gov	An institution that has received data shall allow users to query when this data was accessed and is required to document conformance to the initially published usage policies.

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

sha_10	org, gov	An institution that has received data shall allow users to later revoke consent for provided data.

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

4 Conclusions

This document outlined the requirements identified in the initial design phase of the DIP 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 Del 2.2 Design Document.

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

Appendix

Glossary

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

Abbr.	Definition
DIP	Digital Immunization Passport
DID	Decentralized Identifier
VC	Verifiable Credential
OCA	Overlays Capture Architecture
TDA	Trusted Digital Assistant
PDS	Personal Data Store
GLEIF	Global Legal Entity Identifier Foundation (https://www.gleif.org/en/)
SPECIAL	Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance (project website: https://www.specialprivacy.eu/)

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498