Impulse

Identity Management in PUbLic SErvices

D2.8 IMPULSE architecture specification V2

Lead Author: Jiri Musto (LUT)

With contributions from: ALiCE, GRAD, ICERT, TREE

Reviewers: UC/IC, GRAD

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Delivery date:	28-02-2023
Version:	1.0
Total number of pages:	26
Keywords:	Software architecture, software requirements, electronic identity, e-ID

Executive summary

This deliverable is the second version for the architecture specification and works as an update for the deliverable D2.7. The goal of this deliverable is to present the high-level design of the IMPULSE solution with the help of architectural requirements and views. The changes that have been made to the IMPULSE solution after the first architecture specification (D2.7) are shown and described in this deliverable.

While this is the final architectural specification within the scope of this project, the IMPULSE solution may experience minor changes before and after the second round of pilots held between May 2023 – July 2023.

Document information

Grant agreement No.	**101004459**	**Acronym**	**IMPULSE**
Full title	**Identity Management in PUbLic SErvices**		
Call	DT-TRANSFORMATIONS-02-2020		
Project URL	https://www.impulse-h2020.eu/		
EU project officer	Giorgio CONSTANTINO		

Deliverable	**Number**	D2.8	**Title**	IMPULSE architecture specification – V2
Work package	**Number**	WP2	**Title**	Co-creative design and piloting
Task	**Number**	T2.3	**Title**	IMPULSE architecture specification

Date of delivery	**Contractual**	M25	**Actual**	M25
Status	Version 1.0		☒Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)	Jiri Musto (LUT), Alejandro Cuenca (GRAD), Daniel Pérez (ALiCE), Gianluca Markos (ICERT), Iria Núñez (ALiCE), Jesús Alonso (TREE), Jaime Loureiro (GRAD), Xavier Martinez (GRAD)			
Responsible author	**Name**	Jiri Musto		
	Partner	LUT	**E-mail**	jiri.musto@lut.fi

Summary **(for dissemination)**	This deliverable is an updated version of the D2.7 that focuses on providing a high-level design of the IMPULSE solution and show the changes that have been made after the previous version. The high-level design includes architectural requirements, models, and views of the solution without going to technical detail on how everything is implemented. The original requirements from D2.7 were divided into categories specifying when they should be completed and this deliverable will examine if the necessary requirements have been completed. This document is not the end for design improvements and the IMPULSE solution may still encounter changes in the scope of this project, as it is necessary to continuously improve the solution based on gathered feedback and possible issues that are encountered.
Keywords	Software architecture, software requirements, electronic identity, e-ID

Version Log

Issue Date	Rev. No.	Author	Change
10.01.2023	0.1	Jiri Musto (LUT)	Initial version based on D2.7
26.01.2023	0.5	Jiri Musto (LUT)	Draft for EAB to review
10.01.2023	0.6	Jiri Musto (LUT)	Improved version based on comments
15.02.2023	0.7	Jiri Musto (LUT)	Version for internal review
17.02.2023	0.8	Marco Vianello & Nicolo Fassa (UCIC)	Document review
23.02.2023	0.9	Alicia Jimenez (GRAD)	Document revision
24.02.2023	1.0	Jiri Musto (LUT)	Document finalized

Table of contents

Executive summary 2
Document information 3
Table of contents 4
List of figures 5
List of tables 6
Abbreviations and acronyms 7
Definitions 8
1 Introduction 9
1.1 Background 9
1.2 Aim of this deliverable 9
1.3 Overview of the IMPULSE e-ID solution 9
1.3.1 Registration of the e-ID (enrolment or onboarding) 10
1.3.2 Use of the e-ID (authentication) 11
2 Architectural analysis 12
2.1 Stakeholders, needs, and concerns 12
2.2 Constraints of the project context and environment 13
2.3 Architecturally significant requirements (ASRs) 13
2.3.1 Functional ASRs (features) 14
2.3.2 Non-functional ASRs (quality attributes) 15
3 Architectural design 18
3.1 Main design decisions 18
3.2 Operational view 20
3.3 Deployment view 22
3.4 System integration 23
3.5 Future considerations 24
4 Conclusions 25
References 26

List of figures

Figure 1: Entities or organizations involved in the SSI scheme of IMPULSE.. 10
Figure 2: Architectural views covered in the specification deliverables of IMPULSE WP2 (D2.7-D2.8)..... 18
Figure 3. Operational view of IMPULSE... 21
Figure 4. Deployment view of IMPULSE.. 22
Figure 5. General Integration of a PA with the IMPULSE solution (from D2.9). 23

List of tables

Table 1: List of stakeholders (internal and external to IMPULSE). 12
Table 2: Needs and concerns of citizens (based on pilot results). 13
Table 3: Contextual and environmental constraints of the IMPULSE e-ID solution 13
Table 4: List of functional ASRs. 14
Table 5: List of non-functional ASRs. 16
Table 6. List of main design decisions adopted by the IMPULSE partners 19

Abbreviations and acronyms

- **AI:** Artificial intelligence
- **ASR:** Architecturally significant requirement
- **BC:** Blockchain
- **DID:** Decentralized identifier
- **DLT:** Distributed ledger technology
- **e-ID:** Electronic identity/identification
- **EBSI:** European blockchain service infrastructure
- **eIDAS:** Shorthand for "electronic Identification, Authentication and Trust Services". Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- **ESSIF:** European self-sovereign identity framework
- **FR:** Functional requirement
- **IDM:** Identity management
- **IDP:** Identity provider
- **ML:** Machine learning
- **MRZ:** Machine-readable zone
- **OCR:** Optical character recognition
- **PA:** Public administration
- **QA:** Quality attribute (non-functional requirement)
- **REST:** Representational state transfer
- **RP:** Relying party
- **SP:** Service provider
- **SSI:** Self-sovereign identity
- **SSO:** Single sign-on
- **TI:** Trusted issuer
- **UI:** User interface
- **VC:** Verifiable credential
- **VP:** Verifiable presentation
- **WP:** Work package (IMPULSE project)

Definitions

- **Architecturally significant requirement:** A subset of functional and non-functional requirements that outlines the most significant decisions for the high-level design of the software, which are usually related to key technology choices (e.g. choices of frameworks and dependencies) or the overall structure (e.g., monolithic deployment unit vs microservices) (Brown, 2018).

- **Software architecture:** The set of fundamental concepts and properties of a program or computing system within its environment, represented through the abstraction of its constitutive elements, the relationships among those elements, as well as the principles and choices guiding its overall design and evolution (Rozanski and Woods, 2012; Bass, Clements and Kazman, 2013; Brown, 2018).

- **Stakeholder:** People for whom the system is built, or who are directly or indirectly concerned about it (Rozanski and Woods, 2012; Bass, Clements and Kazman, 2013).

- **View:** In software architecture, the term “architectural view” or simply “view” is used to describe the representation of a coherent set of architectural elements (Bass, Clements and Kazman, 2013), which are depicted from a certain perspective that emphasizes one or more key concerns of the software, such as its structure, its behaviour, or its dependencies. By implication, each view is aimed at specific groups of stakeholders to whom those concerns are important (Rozanski and Woods, 2012).

- **Viewpoint:** The description of the scope, target audience, legend, notation, conventions, or symbols in the diagrams, which altogether serve as a template to construct and interpret a view (Rozanski and Woods, 2012).

1 Introduction

1.1 Background

This architecture specification deliverable (D2.8) reflects the plans to improve IMPULSE based on the first round of pilots held in 2022. Deliverable D2.7 acts as the basis for this deliverable, as D2.8 is the second version of the IMPULSE architecture specification. The purpose of this deliverable is to outline the high-level software architecture design after the first but before the second round of pilots.

This deliverable will follow the same structure as the previous version and has the following three activities: Architectural analysis, architectural design, and architectural evaluation. This version of the architecture specification focuses on the first piloting results as well as what changes have been done or will be done to the IMPULSE architecture. As the previous version outline several architectural requirements, this version will follow up with the requirements to see what have been implemented and what have been changed or even removed by the technical partners.

1.2 Aim of this deliverable

This deliverable aims at providing to general audiences (including non-technical stakeholders, such as citizens, public administrators, policymakers, etc.) a comprehensive view of the high-level software architecture design of the e-ID solution proposed by IMPULSE:

- What are the main features and use cases of the e-ID solution?
    - What are the relevant architectural requirements?
- What is the scope or boundary between the e-ID solution and other software systems or platforms?
- How should the proposed e-ID solution be instantiated, fine-tuned, and deployed to each one of the pilot case environments?
    - What kind of integrations to other systems, internal and external to the public administrations or the rest of the IMPULSE consortium, are required for the functioning of the e-ID solution?

1.3 Overview of the IMPULSE e-ID solution

IMPULSE is an e-ID system that can be integrated into online public services. The system acts as a single-sign-on (SSO) software solution that allows citizens to access the integrated online services. IMPULSE aims to provide an alternative solution to existing e-ID systems by utilizing facial recognition for the sign-up and log-in process to provide easier usage and better security than just a username and password. IMPULSE follows the ESSIF governance framework that is GDPR compliant and relies on smart contracts that store relevant information.

Figure 1 shows the self-sovereign identity (SSI) scheme of IMPULSE, which is similar to other SSI implementations. The solution relies on the blockchain technology to verify users' credentials without needing a central trust authority.

Under the SSI architecture, the user's e-ID is stored in the user's own mobile device in the form of a "verifiable credential" (VC), which contains a special type of persistent identifier called "decentralized identifier" (DID) [1][2]. While the VC remains always in the user's own device, only the DID is saved to the blockchain, so that it can be later used as a proof of integrity for the e-ID. Possible privacy issues related to this architecture are currently under consideration within the ESSIF framework and IMPULSE will follow the updates to be aligned with their identity model.

[1] https://www.w3.org/TR/did-core/

[2] https://www.w3.org/TR/did-use-cases/

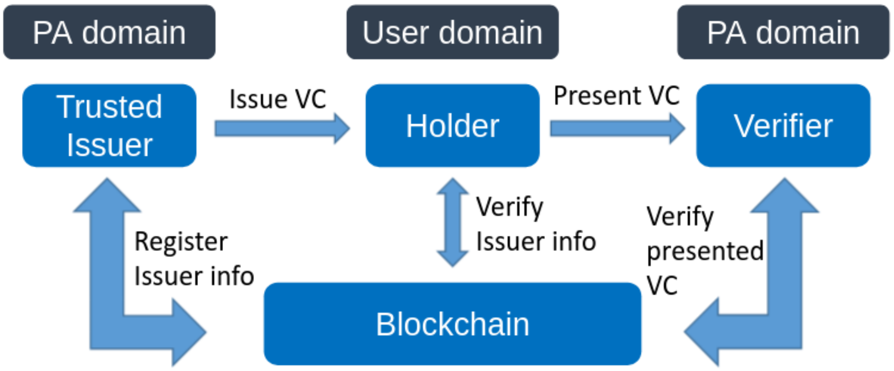

Figure 1: Entities or organizations involved in the SSI scheme of IMPULSE.

By combining three existing and disruptive technologies, namely Artificial Intelligence (AI), Blockchain (BC) and Smart Contracts (SC), IMPULSE aims to transform the two critical processes required to access the online public services: Enrolment and authentication. These are the same two basic workflows or scenarios considered for the design and implementation of the IMPULSE e-ID solution:

1. **Registration of the e-ID (enrolment or onboarding):** Through this digital onboarding process, users request for the first time their identity VC, which will be used later to authenticate to the online public services.
2. **Use of the e-ID (authentication):** Users present their identity VC in order to authenticate to the online public services.

The delivery of the online public service is not handled by IMPULSE solution but it is closely related to the overall IMPULSE experience as the online public service acts as the target where the user tries to log in to.

The following subsections explain the sequence of steps for each one of basic two scenarios handled by IMPULSE. For a more technical description of the processes, there are technical documentation provided by the WP5 in the project.

1.3.1 Registration of the e-ID (enrolment or onboarding)

The onboarding process has the following steps with the IMPULSE solution:

1. User is asked to sign up for the public service.
2. User needs to provide personal information as well as take photos of a valid identification document, such as a national ID or passport.
    a. In the first version of IMPULSE, the personal information is manually written by the user.
    b. In the second version of IMPULSE, the aim is to automatically extract the personal information from the provided document.
3. After the information has been provided to the solution, the user is asked to take a picture of their own face (a selfie)
4. The solution will then compare the selfie with the image in the provided identification document.
    a. Either the selfie and image are verified to be the same or disapproved
5. If the verification is correct, a DID is generated and registered in the chosen blockchain.
6. Now the user has an e-ID that can be used whenever they want to log in to the public service.

The e-ID for the user is stored as a VC in the user’s own mobile device and the VC contains a reference to the same DID that was registered in the blockchain.

1.3.2 Use of the e-ID (authentication)

The authentication (login) process with the IMPUSE solution is similar to the onboarding process but it involves fewer steps to be done by the user and the system:

1. User is asked to log in for the public service.
2. User takes a selfie and the solution checks if there are any existing VCs based on facial recognition.
3. If there are valid VCs, user selects an existing credential and uses that to log in to the public service.

As can be seen, the onboarding process has more steps than the authentication process. This is the case regardless of the public service being accessed with the IMPULSE solution.

2 Architectural analysis

This section presents the factors that provide a starting point and drive the software architecture design, namely: The stakeholders, their needs, and their concerns, together with other contextual or environmental constraints that are externally imposed upon the project. The aforementioned factors (i.e., problem domain) are translated into an actionable set of requirements (i.e., solution domain), formulated from the perspective of the software system features and characteristics.

2.1 Stakeholders, needs, and concerns

Table 1 presents the stakeholders that interact with IMPULSE. The table has been taken from D2.7 as the stakeholders have remained the same throughout the project.

Table 1: List of stakeholders (internal and external to IMPULSE).

Stakeholder name (as Role)	Internal or external to IMPULSE consortium	Description	Individual or organization	IMPULSE selection (if known), other examples
Technical (development) partner	Internal	Designs and develops the e-ID solution	Organization	GRAD, ICERT, ALiCE, TREE, CEL
PA as Service provider (SP)	Internal	Offers online public services to end users	Organization	ARH, ERTZ, GIJON, MOP, RVK, UC/IC
PA as Trusted issuer (TI)	Internal	Issues the VC to the end user	Organization	ARH, ERTZ, GIJON, MOP, RVK, UC/IC
PA as Relying party (RP)	Internal	Verifies the validity of the end user's VC	Organization	ARH, ERTZ, GIJON, MOP, RVK, UC/IC
End user / Citizen / Natural person / Holder of VC	External	Manages its own personal VC to access the service provided by the PA	Individual	-
Blockchain infrastructure provider	External	Offers the SSI governance framework and the underlying blockchain DLT	Organization	EBSI
External software vendor / Technical tender	External	Adapts the IMPULSE e-ID solution to the specific use case of the PA and integrates it into the PA's systems	Organization	See D2.1, Table 3. Other vendors to be selected through public tenders in Spring 2022

Each stakeholder group has a unique set of needs and concerns, which shall be addressed by the IMPULSE e-ID solution. The needs and concerns are different than simply listing anything that the stakeholder "wants": It should refer to the goals that the stakeholder wants to achieve (the jobs-to-be-done) and should be technically, legally, and ethically feasible to achieve those intended goals. Unlike software requirements, the needs and concerns belong to the problem domain.

Table 2: Needs and concerns of citizens (based on pilot results).

Requirement type	High-level goal (D2.2): Evaluation criteria (D2.1)	Concern (D2.4)
Functional	Compliance to legal regulations, technical, and ethical standards	No description of privacy policy or how data is stored.
Functional	Compliance to legal regulations, technical, and ethical standards	No information what data the application is sending to the system (minimization principle of GDPR should be followed).
Functional	Usability and user friendliness: Efficiency, productivity	Lack of information during the onboarding process.
Functional	Technical robustness: Reliability, accuracy	No alternative for facial recognition in case of issues.
Non-Functional	Trustworthiness: Security and fraud prevention	Security concerns with the reliability of facial recognition technology

Table 2 presents the concerns of the citizens (end users) that were identified during the first piloting round and repeated in each case site. Most participants described that the onboarding process was the most difficult part while the log in process was relatively easy-to-use. A more detailed report regarding the pilot results can be found from deliverables D2.4 and D2.11.

2.2 Constraints of the project context and environment

This section lists the limitations, restrictions, or constraints that are imposed upon the project due to external factors, which do not depend on and/or cannot be bypassed the project partners implementing the IMPULSE e-ID solution. Examples of such constraints might be related to the current state-of-the-art of the selected technologies, legal and regulatory framework, or time and resource limitations.

Table 3: Contextual and environmental constraints of the IMPULSE e-ID solution

Const. ID	Categories	Description	Proponent
CC-01	Device compatibility Face Verification	The on-device face verification will require Android devices with version 8.1 or higher.	AliCE

As Table 3 shows, there is currently only one constraint with the IMPULSE solution. The verification API is developed to work with Android devices and while majority of mobile users worldwide are using a compatible phone, there is more than a third of possible users that have an incompatible device. For future development, it would be desired that the IMPULSE solution could work on any operating system as that would enable everyone to start using it.

2.3 Architecturally significant requirements (ASRs)

Architecturally significant requirements (ASRs) are the subset of system requirements that have a significant impact or effect on the software architecture. Some indicators of this impact or effect are:

- The requirement pervades through the whole design
- The requirement is risky
- The requirement has a very high business value or cost of opportunity
- The requirement is non-negotiable
- The requirement is very difficult to change later in the project

Examples of ASR are (1) notifications that inform the user of a process status or (2) possibility to remove data from the software. On the other hand, the formatting or layout of the user interface (UI) are not ASRs, since they can be implemented relatively easily, with few dependencies on other parts of the system, or without the need for major modifications in the overarching distribution of software components and/or the underlying hardware infrastructure.

ASRs can be divided into two categories: **functional** and **non-functional**. Functional ASRs are tangible operations the system does, while non-functional ASRs are qualities of the operations performed by the system. For example, a functional ASR could be to provide information in plain text and the language can be changed and non-functional ASR defines what languages are supported.

2.3.1 Functional ASRs (features)

Table 4 summarizes the minimum essential tasks that the system must perform during runtime, The ASRs have been sorted by their priority, based on the "MoSCoW" method:

- **Must do:** Functionalities that are essential for the proper operation of the IMPULSE e-ID solution and that must be fully implemented, in order to run the 1st round of pilots
- **Should do:** Functionalities that are expected in either the 1st round or the 2nd round of pilots, but which will eventually need to be implemented nevertheless
- **Could do:** Optional or value-adding functionalities that may be expected for the 2nd round of pilots, if time and resources permit it

Compared to the D2.7 version of the table, an additional column has been added to identify if the particular ASR has been completed by the first round of pilots.

Table 4: List of functional ASRs.

Req. ID	Categories	Description	Priority	Done by pilot 1
FR-01	Onboarding Document verification	The system shall recognize that the user's identity card or passport is legitimate (real)	Must do	Done
FR-02	Onboarding Document verification	The system shall recognize that the user's identity card or passport is valid (has not expired)	Must do	In progress
FR-03	Onboarding Document verification	The system shall recognize that the received identity card or passport belongs to the user	Must do	Done
FR-04	Usability Document verification	The system should request a new image of the identity card or passport if the quality of the recognized text is not enough to perform the validation process	Must do	Done
FR-05	Onboarding Face Verification	The system shall verify that the user's face photo (selfie) matches the face from the picture in the ID document	Must do	Done
FR-06	Onboarding Management of VCs	The system shall generate a VC, based on the photos of the user's face and the identity card or passport	Must do	Done
FR-07	Management of VCs	The system shall store the user's VC and the public-private key pair in the user's own mobile device	Must do	Done
FR-08	Management of VCs	The system shall store the decentralized ID (DID) of the user in the blockchain	Must do	Removed
FR-09	Authentication	The system shall verify that the user who is trying to authenticate is the owner of the VC	Must do	Done
FR-10	Authentication	The system shall check against the blockchain that the user's VC has not been tampered with	Must do	Done
FR-11	Authentication	The system shall send a SIOP authorization request to the PA in charge of the requested online service	Must do	Done

Req. ID	Categories	Description	Priority	Done by pilot 1
FR-12	Usability Transparency Regulatory compliance	The system should inform the user about the status of the registration (onboarding) process	Must do	Done
FR-13	Usability Transparency Regulatory compliance	The system should inform the user about the status of the authentication process	Must do	Done
FR-14	Security	The system shall allow users to control their data in a self-sovereign manner	Should do	Done
FR-15	Security	The system shall protect identity information (e.g., ID document, facial, gender, location) that are most critical	Should do	In progress
FR-16	Transparency Regulatory compliance	The user should be able to consult and request the deletion of their off-chain data	Should do	Done
FR-17	Authentication Usability Transparency Effectiveness and reliability	The system should identify the reasons for failure of the authentication process and communicate them to the user.	Should do	Done
FR-18	Management of VCs	The system shall provide the option to choose a particular e-ID if the user has multiple VCs stored on his or her device when logging to a public service	Could do	Done
FR-19	Authentication Face verification	The system shall match the user's face photo (selfie) to an existing VC stored in the device	Could do	Done

As the Table 4 shows, there is one requirement that has been removed from the original list. Requirement FR-08 conflicts with the GDPR which is why it has been removed. Most **Must do** functionalities have been completed aside from FR-02. In addition, while the FR-17 has been completed, during the first pilot round some users encountered a complete lack of any kind of notification, regardless if the authentication process was successful or not. This means that the requirement needs to be modified to consider all possible notifications or an additional requirement has to be added to the list.

Additionally, based on the piloting concerns shown in Table 4, a new functional requirement should be added for the privacy policy information. An alternative log in method needs to be carefully considered in the future in case of issues with the facial recognition, for example cameras not working properly, but it should not be added as a functional requirement before the possible implications have been thoroughly explored.

2.3.2 Non-functional ASRs (quality attributes)

Table 5 summarizes how the system is expected to behave while conducting its essential tasks. Non-functional ASRs generally refer to some overall quality attribute of the system, often expressed using words that end in "-ility", such as reliability, usability, or interoperability. Non-functional ASRs should clearly indicate a metric, acceptable range, or test, which allows to verify whether the quality attribute has been met at the expected level of definition.

The ASRs have been sorted by their priority, based on the "MoSCoW" method:

- **Must do:** Essential software attributes, expected behaviour and/or metrics that must be met by the IMPULSE e-ID solution, in order to run the 1st round of pilots
- **Should do:** Software attributes or metrics that must be met by the IMPULSE e-ID solution, in either the 1st round or the 2nd round of pilots
- **Could do:** Optional or value-adding attributes and metrics (e.g., optimizing use of resources, refactoring, addressing technical debt) that may be fulfilled by the IMPULSE e-ID solution during the 2nd round of pilots, if time and resources permit it

Table 5: List of non-functional ASRs.

Req. ID	Categories	Description	Priority	Done by pilot 1
QA-01	Face verification Effectiveness and reliability	False Acceptance Rate (FAR) <= 1%: Out of 100 authentication requests, up to 1 time the "wrong person" may be authenticated even though it should have been rejected (false positive)	Must do	In progress
QA-02	Face verification Effectiveness and reliability	False Match Rate (FMR) <= 1%: Same concept than FAR but related to face-match. Out of 100 face-matches, up to 1 may be recognized as a match (the score between selfie and ID photo is above the designated threshold), even though it should have been rejected (with score below the threshold), because there are not enough similarities between the ID photo and the selfie	Must do	In progress
QA-03	Document verification Effectiveness and reliability	The system should be able to recognize text from images of identity cards or passports of varying quality, illumination, resolution and focus	Must do	In progress
QA-04	Data protection Regulatory compliance Security	The public key should be stored in BC only as hash value and anyway it must never be possible to trace back from the public to the private key	Must do	Removed
QA-05	Data protection and security	The system should prevent unauthorized third parties from accessing any user's personal data	Should do	Done
QA-06	Data protection and security	Biometrics and other personal identity data should be encrypted	Should do	To be done
QA-07	Face verification Usability	The system should be able to recognize faces captured from images with different resolutions and illumination	Should do	Done
QA-08	Usability Transparency	The system should provide basic instructions (of the mobile app) in a language that is simple and clear to the user	Should do	Done
QA-09	Onboarding Usability Transparency	The system should provide simple and well-guided user actions when collecting image samples for face recognition	Should do	Done
QA-10	Authentication Usability	The system should reduce cognitive burden (remembering many user accounts and passwords) for users.	Should do	Done
QA-11	Face verification Effectiveness and reliability	True Positive Rate (TPR) > 75%: The system should accept the "right user" to authenticate at least 76 out of every 100 times	Should do	In progress
QA-12	Face verification Effectiveness and reliability	False Rejection Rate (FRR) <= 25%: Out of 100 authentication requests, up to 25 may be denied even if the user is really who she claims to be (false negative)	Should do	In progress
QA-13	Document verification Effectiveness and reliability	True Positive Rate (TPR) > 75%: The system should accept genuine identity cards or passports at least 76 out of every 100 times	Should do	In progress
QA-14	Document verification	False Acceptance Rate (FAR) <= 1%: Out of 100 identity card or passport validation	Should do	To be done

Req. ID	Categories	Description	Priority	Done by pilot 1
	Effectiveness and reliability	requests, up to 1 time a forged or tampered identity card or passport may be accepted even though it should have been rejected (false positive)		
QA-15	Data protection Regulatory compliance Transparency	The SC should ensure a plain oversight and control by the users over the consent management process (provide the chance to withdraw the consent).	Should do	In progress
QA-16	Data protection Regulatory compliance Usability Transparency	The system should provide informed consent in a legal language and accessible with dedicated icons.	Should do	In progress
QA-17	Security Transparency	The system should indicate users where their personal data is stored.	Should do	Done
QA-18	Portability and availability	The system should allow to authenticate users at any place and anytime if Internet connection is available and the IMPULSE solution services are up.	Could do	Done

As Table 5 shows, there is one non-functional ASR that has been removed (QA-04). This was removed because the requirement was completely wrong. To be GDPR compliant, the public keys of legal entities are stored in the ledged publicly while the public keys of the natural person are not. There are also three **Must do** requirements that were not completed (QA-01, QA-02, QA-03) before first piloting round but they are to be completed for the second piloting round. Especially the QA-03 will improve the onboarding process that most users found to be cumbersome and it will also resolve the FR-02 requirement.

For information regarding the facial recognition verification reliability and effectiveness (QA-07, QA-11, QA-12) can be found here[3].

[3] Alice Biometrics NIST report: https://pages.nist.gov/frvt/reportcards/11/alice_000.html

3 Architectural design

This chapter summarizes the essential features of the IMPULSE e-ID solution architecture. It begins with a list of the key design decisions that have been adopted by the technical partners of the Consortium, in order to address certain requirements or constraints of the project, prior to the execution of the first piloting round. This is followed by a set of diagrams (i.e., architectural views), which illustrate the high-level design of the IMPULSE system architecture from a "black box" (context) and "white box" (functional) perspective.

Figure 2 outlines the scope of the different views that will be covered in the two iterations of the architecture specification deliverables of WP2 (D2.7-D2.8). The views marked in yellow refer to key aspects of the software design that are transparent or agnostic to the environment of the pilot cases. The views marked in light blue refer to key aspects that are related to or depend on the integration and instantiation environment of each pilot case (even if the IMPULSE e-ID solution is always the same, the configuration of actors, hardware, and software elements surrounding the e-ID solution can differ). Both the yellow and light blue boxes refer to views covering the high-level software design and addressing key aspects that concern a wide set of project stakeholders, such as public administrations, policymakers, and citizens.

The views marked in dark blue refer to key aspects that concern primarily the technical partners implementing the solution. These views may also reveal lower-level details that are protected by the individual partner organizations' IP rights under the IMPULSE Consortium grant agreement. Consequently, the views marked in dark blue remain outside the scope of the public architecture specification deliverables of WP2.

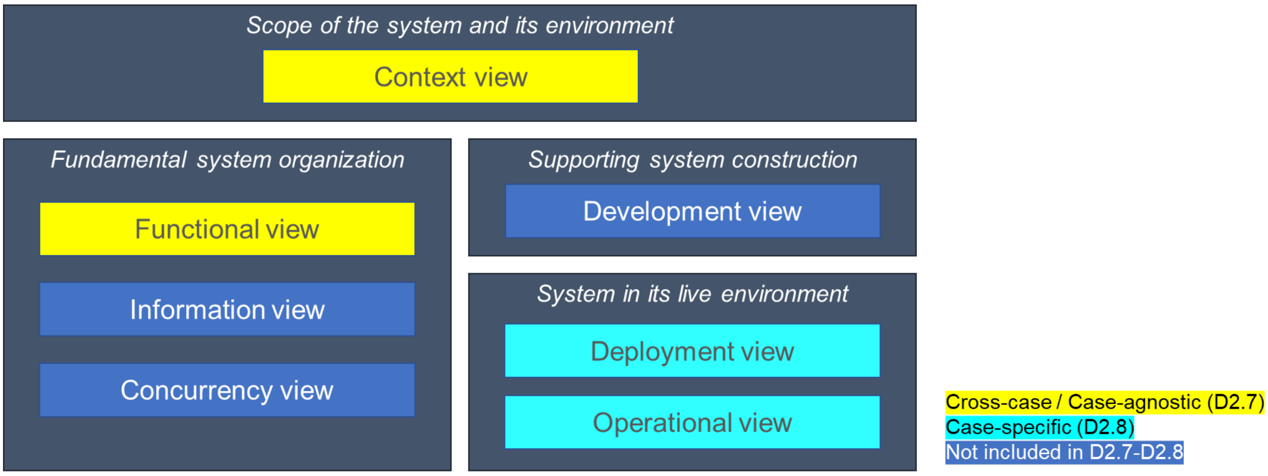
Scope of the system and its environment
Context view
Fundamental system organization
Functional view
Information view
Concurrency view
Supporting system construction
Development view
System in its live environment
Deployment view
Operational view
Cross-case / Case-agnostic (D2.7)
Case-specific (D2.8)
Not included in D2.7-D2.8

Figure 2: Architectural views covered in the specification deliverables of IMPULSE WP2 (D2.7-D2.8)

3.1 Main design decisions

There are key decisions consciously taken by the project partners which can have a significant impact or influence over the design of the software architecture. The design decisions have been presented in D2.7 but there have been some additions and modifications to the original list. These changes are presented in Table 6 with a bolded text. The design decisions are a result of attempting to solve specific ASRs or project constraints.

Table 6. List of main design decisions adopted by the IMPULSE partners

Decision ID	Brief description and rationale	ASR or constraint from which this decision originates (if applicable)	Possible risks or trade-offs
DD-01	Selection of EBSI/ESSIF as provider and framework for blockchain infrastructure.		Saving costs of licensing and/or usage of infrastructure provided by a private vendor (+). Binding the IMPULSE piloting roadmap and the development status of the e-ID solution to the EBSI timeline (-).
DD-02	Review of identity document images by a civil servant, in case of positive detection of forgery.	QA-14	Access can still be guaranteed in case the document verification module gives a false negative (+). **It follows the current eIDAS regulation (+).** Slower access to the solution (-).
DD-03	Restriction of identity document types accepted by the system to: National ID card (GIJON, ERTZ, MOP, UC/IC) or passport (ARH, RVK).		Better performance for the selected types (+). Enabling the retrieval of a unique identifier (e.g., national identity code) per each user or the e-ID solution (+). Lesser variety of accepted ID documents (-).
DD-04	Asynchronous communication between the document verification service and the enterprise service of IMPULSE (Estimated time: 1-2 minutes).		Lower waiting times and better user experience overall (+). Decreased user experience and additional steps in the registration / onboarding workflow (-). Feedback regarding errors in the process is not provided live to the users (-) Longer waiting times outside the app might cause the user to abandon the registration (-).
DD-05	**Notifications about the availability of the identity verifiable credential are sent via the decentralized EBSI notification system.**	DD-01	**System does not rely on a unique third party for the notifications, eliminating a point of dependency and centralization (+).** **EBSI notification system does not require any additional configuration as it uses the same DIDs of the PAs and users for sending/receiving the notifications (+).** **EBSI notification system is slower than common PUSH notifications (e.g. Firebase notifications) (-).**
DD-06	**Implementation of the EBSI DID Method v2**		**Greater user privacy (+).**

Decision ID	Brief description and rationale	ASR or constraint from which this decision originates (if applicable)	Possible risks or trade-offs
	(DID of the person not stored in the EBSI ledger)		**It follows the GDPR (+).** **It requires less communication so it is faster (+).** **Persons cannot rotate their keys maintaining their DID; they have to create a new DID (-).**
DD-07	A list of VCs, showing only the VC's name, is available without face recognition.	FR-10	Each VC can be linked with a different biometric profile (+). **The number of credentials and the name of each credential can be seen by someone who has access to the user's device (-).**
DD-08	The app uses the language configured as primary in the smartphone. If translations are not available for this language, English is used by default. In any case, the selected language is configurable from those available.	QA-04	Easier setup (+). **Only Spanish, Icelandic, Italian, Bulgarian, Danish and English are supported (-).**
DD-09	Use of standard VC schemas instead of ad-hoc schemas.	FR-05	Interoperability, reliability on the claims that must be present in the VC (+). VC cannot contain specific claims that are not in the standard schema, even if we do not expect this to be a need (-).
DD-10	**Dockerization of Enterprise Service**		**Easier to deploy in any Public Administration infrastructure. (+)** **Not every Public Administration IT team might have experience in the deployment of containers (-)**

3.2 Operational view

The operational view should provide a solution-free description of the operations related to the software. Figure 3 presents the operational view of the IMPULSE solution.

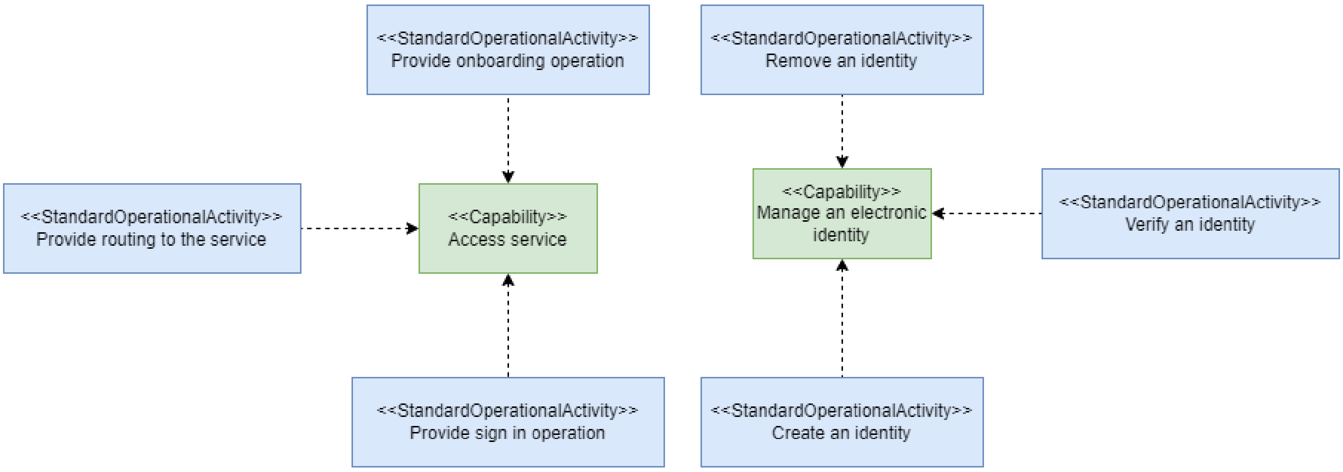
<<StandardOperationalActivity>>
Provide onboarding operation
<<StandardOperationalActivity>>
Remove an identity
<<StandardOperationalActivity>>
Provide routing to the service
<<Capability>>
Access service
<<Capability>>
Manage an electronic identity
<<StandardOperationalActivity>>
Verify an identity
<<StandardOperationalActivity>>
Provide sign in operation
<<StandardOperationalActivity>>
Create an identity

Figure 3. Operational view of IMPULSE

As the Figure 3 shows, the IMPULSE solution has two main capabilities that are provided:

1. Access to the service, provided by the public administration
2. Management of the electronic identity

Both capabilities have specific operations that should be possible to do. The service access requires an operation to onboard, sign in, and route to the service. These operations are mandatory for IMPULSE solution to be able to function. Similarly, the management of an electronic identity has three operations that are vital for IMPULSE: creating, verifying, and removing an identity. All of these operations are implementation-free, and each public administration can have their own implementation to provide the specified operations. For example, the service that is accessed is different for each public administration, thus there may be some differences on how the routing is handled within the implementation.

3.3 Deployment view

The purpose of the deployment view is to show important parts of the system and to define the environment where the system is intended to run. Deployment view should provide the primary components of the system and their dependencies or connections to each other.

Figure 4 shows the deployment view of the IMPULSE solution.

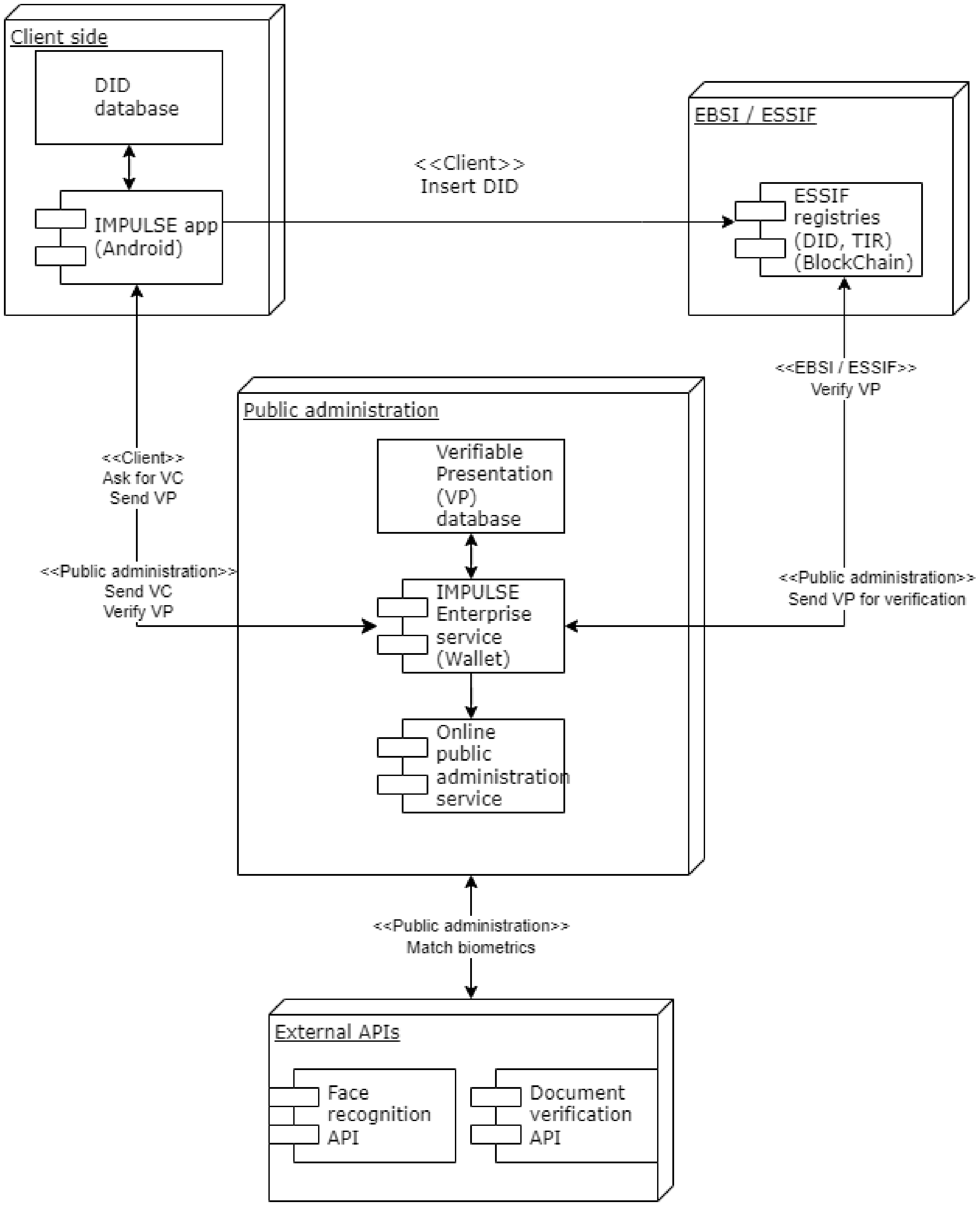
Client side
DID database
IMPULSE app (Android)
<<Client>> Insert DID
EBSI / ESSIF
ESSIF registries (DID, TIR) (BlockChain)
<<EBSI / ESSIF>> Verify VP
<<Client>> Ask for VC Send VP
<<Public administration>> Send VC Verify VP
Public administration
Verifiable Presentation (VP) database
IMPULSE Enterprise service (Wallet)
Online public administration service
<<Public administration>> Send VP for verification
<<Public administration>> Match biometrics
External APIs
Face recognition API
Document verification API

Figure 4. Deployment view of IMPULSE

As Figure 4 shows, there are four main parts to the IMPULSE solution: client, public administration, EBSI / ESSIF and external APIs. Each four parts have their own required components.

- **Client**: Client (or the user) is the person who has IMPULSE installed on their mobile device. When onboarding, the client will request for the VC from the public enterprise service and insert a DID to the EBSI / ESSIF service after they are verified by the enterprise service. This DID will be stored on the mobile device as well for IMPULSE solution to access when the client plans to log in When signing in, the client will send their VP to the enterprise service for verification.

- **Public administration:** The enterprise service managed by the public administration acts as the central point of the IMPULSE solution. Most data will go through the enterprise service during the onboarding or authentication processes. When a client needs to onboard, the identity card and selfie are sent to the enterprise service for verification with the help of external APIs. If the client is verified, the VP is stored in a database on the public administration's site for authentication purposes. When client wants to authenticate for the online public administration service, the enterprise service will ask EBSI / ESSIF to verify the VP and associated DID before allowing the client to log in to the service.
- **EBSI / ESSIF:** EBSI / ESSIF maintain the service where the DID will be stored. The method of creating and storing the DID is defined by EBSI / ESSIF.
- **External APIs:** The external APIs consist of face recognition and document verification APIs. These are responsible to match the biometrics of the client's identity document and selfie and provide the response to the public administration.

3.4 System integration

There are six pilot cases in five different countries that have had IMPULSE instantiated on their site. The pilot sites had their own services the IMPULSE solution should integrate with.

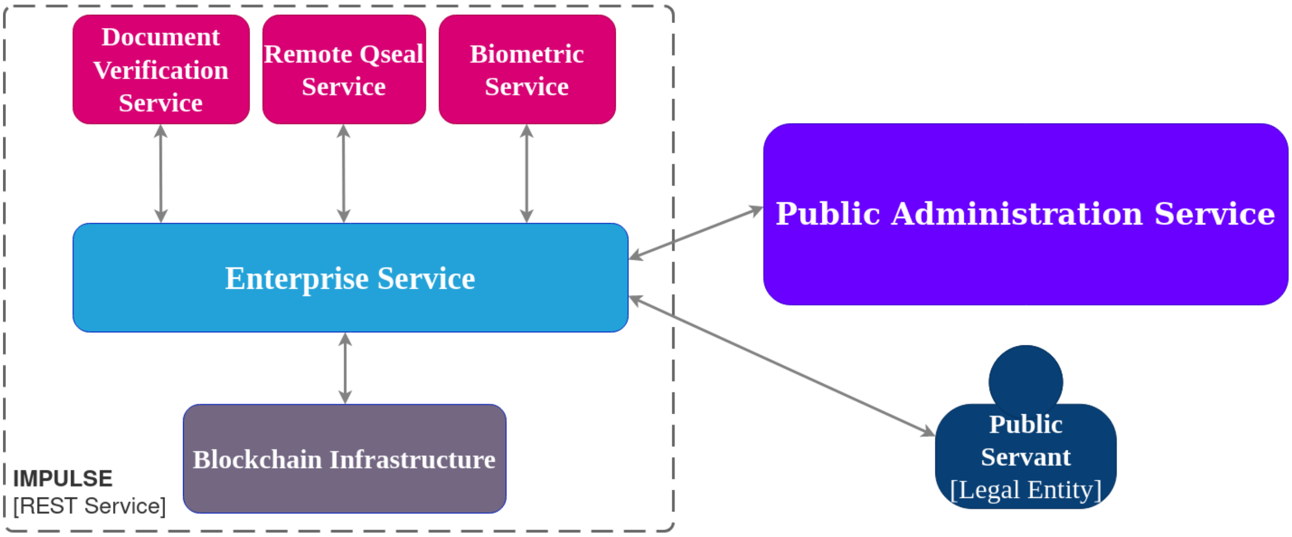

Figure 5. General Integration of a PA with the IMPULSE solution (from D2.9).

Figure 5 presents the general integration of the public administration service with the IMPULSE solution. The image is from deliverable D2.9, which can be read for a more technical overview of the instantiation process.

In most case locations, the instantiation procedure was similar. The different pilot sites had to modify their desired online platform to allow the transmission of messages between the online service and the enterprise service. The main outlier in the pilot cases was ARH as their service included embedded software in a locker. The original plan was to have the enterprise service in the locker to allow users to use IMPULSE solution to be able to open specific lockers. However, the locker supplier was not able to deliver the desired solution on time for the first round of pilots, which lead to having a mock-up version of the idea. The IMPULSE solution was instantiated in the same way as other pilot sites but instead of signing into a service and accessing a web site, the case owner would manually open the locker after verifying the successful authentication.

3.5 Future considerations

At its current stage, IMPULSE solution is reliant on the EBSI / ESSIF. This means that when their service is unavailable, IMPULSE solution will be unusable. If IMPULSE solution could be used with another blockchain service, the solution could be adopted with less restrictions.

While the face recognition and document verification APIs are provided by project members, these APIs could be swapped with other provides as long as the structure of the API requests and responses are modified to be compatible. It could also be possible to utilize multiple APIs for verification if that is deemed to be necessary for improved verification results or if that would increase the availability of the APIs (as backup services).

Finally, the IMPULSE solution works only on Android devices, and this is quite a heavy restriction to users. It would be beneficial if the solution could be extended to be used with Apple devices, as there are close to 30 % iOS users worldwide[4].

[4] Statista 2022, https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

4 Conclusions

This deliverable aimed to provide a high-level software architecture design of IMPULSE and answer the following questions:

- What are the main features and use cases of the e-ID solution?
  - What are the relevant architectural requirements?
- What is the scope or boundary between the e-ID solution and other software systems or platforms?
- How should the proposed e-ID solution be instantiated, fine-tuned, and deployed to each one of the pilot case environments?
  - What kind of integrations to other systems, internal and external to the public administrations or the rest of the IMPULSE consortium, are required for the functioning of the e-ID solution?

These same questions were presented in the first version of the architecture specification (D2.7) and most answers are still similar. IMPULSE has multiple stakeholders with different needs and concerns that need to be considered when developing the solution. The different functional and non-functional ASRs have slightly changed from the initial literacy analysis to the first round of pilots and the IMPULSE solution will still be further improved. There are some requirements that have been initially completed (such as informing the user of the process) but after the first pilot testing it was found out, that these parts need to be re-evaluated. Especially when many users had issues with the lack of information during the on-boarding process with IMPULSE. Some of concerns from the pilot test were planned to be resolved for the second round of pilots before the actual pilot testing and the results reinforced the idea.

There is a limited amount of time between the first and second round of pilots, so new minor requirements may be difficult to be completed on time. The IMPULSE solution will be tested internally once more before the next piloting period to find out other relevant issues that need to be solved.

During the development period, EBSI / ESSIF framework was updated, and the IMPULSE solution had to be modified to make it compatible. If the IMPULSE solution were to use another blockchain service, similar modification would have to be done.

Most pilot locations have a similar service structure and can be instantiated in the same way. The most different pilot location is ARH, where instead of logging into a public service, the plan is to be able to access a locker with the IMPULSE application. During the first round of pilots, there were issues with the delivery of said locker and the case owners had to demonstrate the functionality by opening the locker manually, instead of IMPULSE properly integrating with it.

For future, the IMPULSE solution should not only improve the usability aspects of the solution but also improve the freedom for instantiation. The solution is currently using the EBSI / ESSIF framework and blockchain as well as APIs developed by the consortium partners for facial recognition and document verification. If someone wants to adopt the IMPULSE solution and utilize another blockchain and external APIs, there should be a possibility to adapt different components to the architecture.

Additionally, IMPULSE currently requires a new onboarding for each service, which is also more cumbersome than authentication. It would be beneficial for IMPULSE to be able to use the same existing identity for other services as well, either by providing easier onboarding or a universal identity for the user.

References

- Bass, L., Clements, P. and Kazman, R. (2013) *Software architecture in practice*. 3rd ed. Upper Saddle River, NJ: Addison-Wesley (SEI series in software engineering).

- Brown, S. (2018) *Software architecture for developers - Volume 1*. Leanpub. Available at: http://leanpub.com/software-architecture-for-developers.

- Rozanski, N. and Woods, E. (2012) *Software systems architecture: working with stakeholders using viewpoints and perspectives*. 2nd ed. Upper Saddle River, NJ: Addison-Wesley.