Identity Management in PUbLic SErvices

D2.7 IMPULSE architecture specification V1

Lead Author: José Carlos Camposano (LUT)
With contributions from: ALiCE, GRAD, ICERT, TREE
Reviewers: TREE, MOP

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Delivery date:	29-04-2022
Version:	1.4
Total number of pages:	29
Keywords:	Software architecture, software requirements, electronic identity, e-ID

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459

Executive summary

This deliverable builds upon the requirements specification (D2.2, D2.3), and provides architectural design that is relevant to the implementation of the IMPULSE system and its software components. The design is based on stakeholder analysis and identification of architecturally significant requirements.

The main goal of this task is to illustrate the high-level design of the IMPULSE system architecture and its behaviour in different scenarios of the pilots. The first iteration of the architecture specification (D2.7) describes the software modules and their components, interactions, and message flows between the modules from a cross-case or case-agnostic perspective. The second iteration (D2.8) will expand upon other requirement nodes for the communications and connectivity issues related to each of the pilot cases. The architecture specification will be compliant with existing standards, and it will specify the high-level design of the system.

The IMPULSE architecture specification will be developed iteratively in two steps: The first version (D2.7) for the first basic system prototype of T5.5, as a base for the first piloting round; and the second version (D2.8) for the final IMPULSE system of T5.5, as a base for the second piloting round and subsequent adoption of IMPULSE after the project. The deliverable is structured as follows: background and overview of the IMPULSE e-ID solution, followed by architectural analysis and design.

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**	D2.7	**Title**	IMPULSE architecture specification – V1
Work package	**Number**	WP2	**Title**	Co-creative design and piloting
Task	**Number**	T2.3	**Title**	IMPULSE architecture specification

Date of delivery	**Contractual**	M15	**Actual**	M15
Status	version 1.4		☐Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☐Public ☐Confidential			

Authors (partners)	José Carlos Camposano (LUT), 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**	José Carlos Camposano		
	Partner	LUT	**E-mail**	jose.camposano@lut.fi

Summary (for dissemination)	This deliverable builds upon the requirements specification (D2.2, D2.3) and provides architectural design that is relevant to the implementation of the IMPULSE system and its software components. The main goal of this task is to illustrate the high-level design of the IMPULSE system architecture and its behaviour in different scenarios of the pilots. The first iteration of the architecture specification (D2.7) illustrates the software modules and their components, interactions, and message flows between the modules from a cross-case or case-agnostic perspective. The second iteration (D2.8) will expand upon other requirement nodes for the communications and connectivity issues related to each of the pilot cases. The architecture specification will be compliant with existing standards, such as ESSIF and eIDAS, and it will specify the high-level design of the system. The IMPULSE architecture specification will be developed iteratively in two steps: The first version (D2.7) for the first basic system prototype of T5.5, as a base for the first piloting round; and the second version (D2.8) for the final IMPULSE system of T5.5, as a base for the second piloting round and subsequent adoption of IMPULSE after the project.
Keywords	Software architecture, software requirements, electronic identity, e-ID

Version Log

Issue Date	Rev. No.	Author	Change
22/11/2021	0.1	José Carlos Camposano (LUT), Alejandro Cuenca (GRAD), Jesús Alonso (TREE), Daniel Pérez (ALiCE), Gianluca Markos (ICERT)	Initial list of stakeholders and ASRs

08/12/2021	0.2	José Carlos Camposano (LUT)	Revising and merging contributions from 1st iteration
13/01/2022	0.3	José Carlos Camposano (LUT), Alejandro Cuenca (GRAD), Jesús Alonso (TREE), Daniel Pérez (ALiCE), Gianluca Markos (ICERT)	Stakeholder needs and concerns, prioritization of ASRs, key design decisions
22/02/2022	0.4	José Carlos Camposano (LUT), Alejandro Cuenca (GRAD), Jesús Alonso (TREE), Iria Núñez (ALiCE), Gianluca Markos (ICERT)	Catalogue of functional elements
21/03/2022	0.5	José Carlos Camposano (LUT), Gianluca Markos (ICERT), Jaime Loureiro (GRAD), Xavier Martinez (GRAD)	Finalized context and functional structure views
22/03/2022	1.0	José Carlos Camposano (LUT)	Completed draft for internal review
30/03/2022	1.1	Jesús Alonso (TREE), Georgi Simeonov (MOP)	Official Reviewers comments
08/04/2022	1.2	Jiri Musto (LUT)	Revision based on comments
15/04/2022	1.3	Alicia Jimenez (GRAD)	General review for quality check
22/04/2022	1.4	Jiri Musto (LUT)	Revision based on comments

Table of contents

List of figures

List of tables

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).

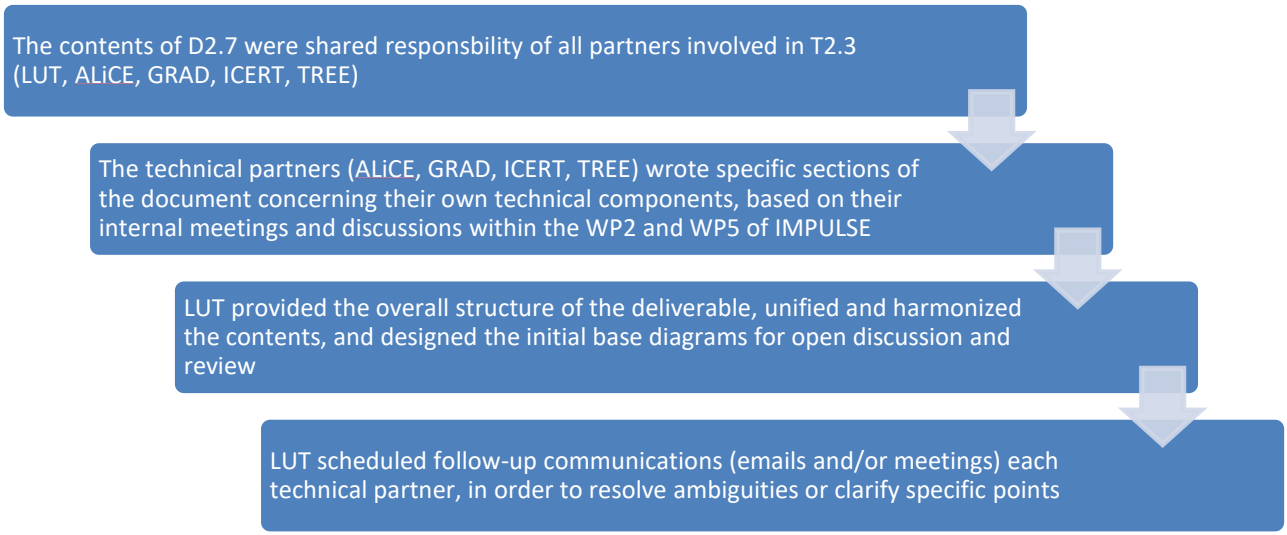
- **View:** In software architecture, the term “architectural view” or simply “view” is used to describe the representation of a coherent set of architectural elements (Bass, Clements and Kazman, 2013), which are depicted from a certain perspective that emphasizes one or more key concerns of the software, 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 deliverable (D2.7) corresponds to the first iteration of IMPULSE's architecture specification (version 1 – V1), which outlines the high-level software architecture design, prior to the first instantiation (D2.9) and the first assessment of the case study pilots (D2.11). The process for the construction of this deliverable is shown below:



This architecture specification deliverable (D2.7) comprise three activities that are interconnected and iterative: Architectural analysis, architectural design, and architectural evaluation.

As shown in Figure 1, the first iteration of the architecture specification (D2.7) focused on the requirements from scientific literature and internal co-creation workshop that were summarized in the requirements specification V1 (D2.3), the initial analysis of the case studies and their stakeholders (D2.1), and the technical specifications of the IMPULSE electronic identity (e-ID) solution according to the project DoA. These sources of input were combined during the first round of architectural analysis and design. The results of this deliverable are the basis to guide the work of instantiation, integration, and adaptation of the IMPULSE e-ID solution to the initial round of pilots in T2.4 and T2.5.

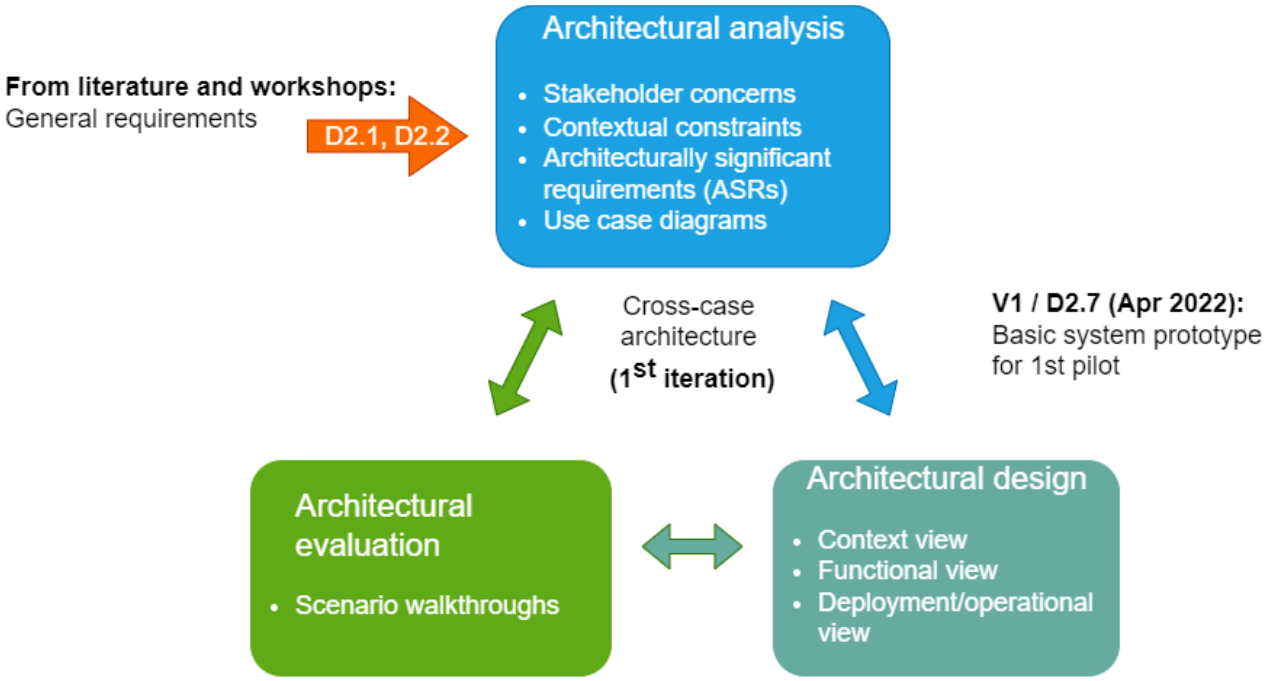


Figure 1: Relationship among the architecture specification V1 and other deliverables of WP2

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. These objectives are summarized through the following research questions and sub-questions:

- How does a new e-ID solution based on the vision and stack of disruptive technologies of IMPULSE work?
    - Who are the main actors that interact directly or indirectly with the e-ID solution?
    - What are the main features and use cases of the e-ID solution?
    - What is the scope or boundary between the e-ID solution and other software systems or platforms?
    - How are the functional responsibilities of the e-ID solution distributed among different components?
- 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?

The first question refers to the high-level, general architecture, which shall be applied across any pilot case implementations, whereas the second question refers to any case-specific considerations that are deemed necessary for the successful local implementation of the proposed solution.

1.3 Overview of the IMPULSE e-ID solution

IMPULSE is a novel e-ID management system that can be integrated as a new option into online public services. It acts as a decentralized single sign-on (SSO) software solution, which can allow citizens to access online public services from different public administrations (PA), also referred to as service providers (SP), by using the camera of their mobile device as authentication mechanism.

e-ID systems manage sensitive and personal data that must be duly protected. IMPULSE proposes an alternative to the existing e-ID management systems that is both more secure and better at preserving the user's privacy. On one hand, through the use of biometrics, IMPULSE provides additional security checks that are harder to bypass than those found in traditional e-ID systems based on single-factor authentication (i.e.,

username and password). On the other hand, IMPULSE gives the user more control over their personal data than those e-ID management systems based on centralized or federated architectures (e.g., Facebook, Google, LinkedIn), because it adopts the concept of self-sovereign identity (SSI) at the core of its user-centric approach to e-ID.

IMPULSE follows ESSIF's governance framework, which relies on smart contracts that store the relevant information (e.g., organizational information about the issuers of credentials). As shown in Figure 2, the SSI scheme of IMPULSE is similar to other SSI implementations, relying on the distributed ledger technology (DLT) commonly known as "blockchain", as a means to verify the users' credentials without the need for 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) [12]. 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.

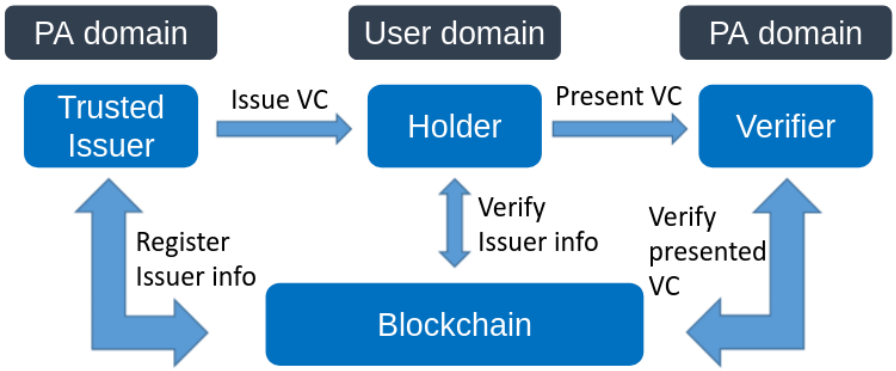


Figure 2: Entities or organizations involved in the SSI scheme of IMPULSE.

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.

A third workflow or process related to IMPULSE, but not directly handled by the e-ID solution, is the delivery of the online public service itself, after the end user has successfully authenticated. Figure 3 illustrates the basic workflow scenarios and entities involved.

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

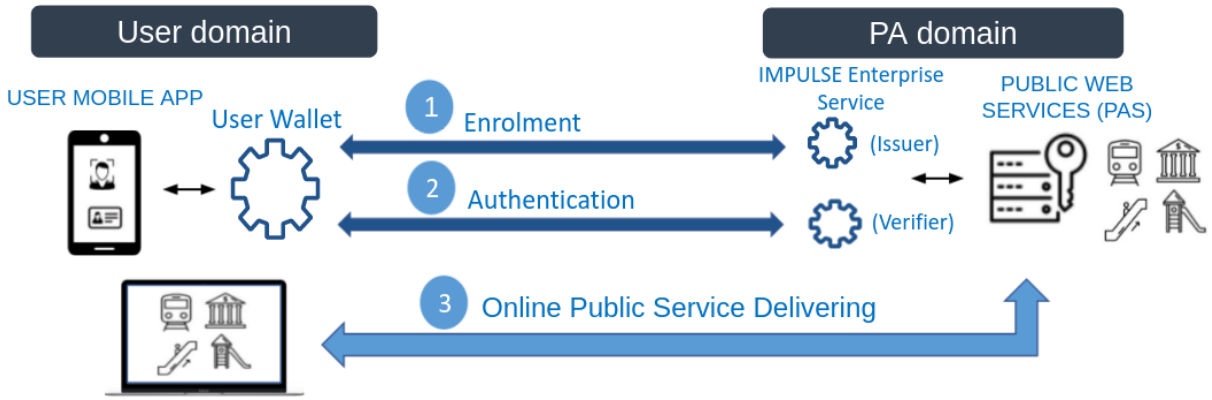


Figure 3: Basic workflows or processes related to IMPULSE.

The following subsections explain the sequence of steps for each one of basic two scenarios handled by IMPULSE.

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

- The user is requested to present an identification document. The document can be a passport or any legally recognized national ID, which must be held and shown in front of the device camera.
  - For the initial round of pilots, each case will choose only one type of ID document (the most common or widely adopted). Additional ID documents will be supported in the second iteration of pilots.
- After the ID document has been scanned, the person takes a selfie of her face. Face biometrics are collected and securely stored.
- The software uses a combination of algorithmic solutions based on biometrics and document verification techniques to check the user's identity.
  - This involves the validation of the ID document itself (document verification techniques) and a perfect match with the holder (facial verification techniques). To prevent fraud, deep learning-based face recognition algorithms are used to compare the user's selfie with the photo on the ID card.
  - Additional security measures for presentation attack detection are applied following the recommendations of the ISO/IEC 30107 standard to guarantee the security of the biometric onboarding.
- Provided that the verification is correct, a DID is generated and registered in a permissioned blockchain managed by a distributed network of nodes.
  - Identities based on the ledger (blockchain) are not under the control of any single identity provider (IDP), but instead the citizen retains the control of her own e-ID, associated personal data, and the rules enforcing the informed consent clauses for processing it. This principle is also known as SSI.
- The e-ID of the user is stored as a VC in the user's own mobile device. The VC contains a reference to the same DID that was registered in the blockchain, so that the user's identity can be verified without the need for a trust authority or identity provider.
- A smart contract between the citizen and the PA/SP may also be established in later iterations of the software solution, in order to enable a more dynamic management of the terms and conditions for processing personal data.

1.3.2 Use of the e-ID (authentication)

- The user requests the access to a public service or resource (this could also apply to private ones under the same criteria). Citizens (or legal entities) can use their newly derived e-ID for authentication.
- The PA/SP verifies the VC's DID in the blockchain and requests the user to prove the ownership of that VC by issuing a challenge.
- The user proves her identity again using real-time face recognition.
- If the identity verification process takes place successfully, the user is forwarded or redirected to the service. Otherwise, access to the service is denied.

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

These refer to the organizations or individuals that will interact with the IMPULSE e-ID solution. The same stakeholder can have multiple roles. Table 1 summarizes the main groups of stakeholders that use, interact, and/or are affected directly or indirectly by the e-ID solution. Some stakeholders may fulfil multiple roles at the same time, such as the public administrations that will also act in the pilot case experiments as SP, TI, and RP, even if in a real production environment, each of these functions could be assigned to different organizations.

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. Consequently, they are generally phrased using the stakeholders' own perspective and language.

Table 2: Needs and concerns of stakeholders (based on D2.1 and D2.2).

Stakeholder role (D2.1)	High-level goal (D2.2): Evaluation criteria (D2.1)	Concern (D2.2)
Functional (Regular users or citizens)	Compliance to legal regulations, technical, and ethical standards Trustworthiness: Resilience to attack, security, and fraud prevention	As a citizen, I want that my personal and biometric data remain protected, so that I am sure that unauthorized third parties cannot access confidential information about me.
Functional (Regular users or citizens)	Trustworthiness: Transparency, understandability, explainability, control and governance of personal data	As a citizen, I want to know where my information is stored and how it is used, so that I can feel it is safe from unauthorized access and/or processing.
Functional (Regular users or citizens)	Usability and user friendliness: Efficiency, productivity	As a citizen, I want to access different public services without the need of memorizing many user accounts and passwords, so that I can reduce the time and cognitive burden.
Functional (Regular users or citizens)	Trustworthiness: Security and fraud prevention	As a citizen, I want to have an easy way to protect or delete the personal data stored in my mobile device if I lose it, so that I am sure that unauthorized third parties cannot access confidential information about me.
Responsibles (PAs)	Technical robustness: Reliability, accuracy	As a responsible, I want to grant access to public services to citizens whose identity has been verified, so that I can prevent unauthorized access and misuse of public resources.
Operators (PAs)	Technical robustness: Cross-border interoperability, mutual recognition, scalability	As an operator, I want to have an interoperable e-ID solution, so that I can easily integrate new services and reach a larger number of users.
Functional (Technical partner)	Compliance to legal regulations, technical, and ethical standards: Control and governance over own personal data Usability and user friendliness	As a technical partner, I want the users to own a smartphone device, so that they can carry their identity information with them instead of having to do the onboarding again (e.g., using a device provided by the PA) every time they want to access a service.
Functional (Technical partner)	Technical robustness: Maintainability, effectiveness / validity / functionality	As a technical partner, I want the users to keep the user app up to date, so that any new functionality can be used.
Functional (Technical partner)	Trustworthiness: Security and fraud prevention	As a technical partner, I want the PAs to manage the system in a secure way, so that the system does not get compromised.
Functional (Technical partner)	Trustworthiness: Security and fraud prevention	As a technical partner, I want the PA to have a fallback method (e.g., manual verification) to check the identity document and biometric information of the user, so that they can accept or reject the onboarding if the facial recognition or the document verification services do not provide decisive results.

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

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

Some examples of things that are not ASRs are the formatting or layout of the user interface (UI), 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.

2.3.1 Functional ASRs (features)

The table below summarizes the minimum essential tasks that the system must perform during runtime, as well as its inputs and outputs. The initial list of requirements comes from the IMPULSE project description and the input from project stakeholders, which was previously collected and summarized in deliverable 2.2 (IMPULSE requirements specification V1).

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

Table 4: List of functional ASRs (based on the requirements specification V1 D2.2).

Req. ID	Categories	Description	Priority	Involved partner(s)
FR-01	Onboarding Document verification	The IMPULSE system shall recognize that the user's identity card or passport is legitimate (real)	Must do	TREE
FR-02	Onboarding Document verification	The IMPULSE system shall recognize that the user's identity card or passport is valid (has not expired)	Must do	TREE

Req. ID	Categories	Description	Priority	Involved partner(s)
FR-03	Onboarding Document verification	The IMPULSE system shall recognize that the received identity card or passport belongs to the user	Must do	TREE
FR-04	Usability Document verification	The IMPULSE 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	TREE
FR-05	Onboarding Face Verification	The IMPULSE system shall verify that the user's face photo (selfie) matches the face from the picture in the ID document	Must do	ALiCE
FR-06	Onboarding Management of VCs	The IMPULSE system shall generate a VC, based on the photos of the user's face and the identity card or passport	Must do	GRAD
FR-07	Management of VCs	The IMPULSE system shall store the user's VC and the public-private key pair in the user's control in the own mobile device, following SSI best practices	Must do	GRAD
FR-08	Management of VCs	The IMPULSE system shall store the DID of the user in the blockchain	Must do	GRAD
FR-09	Authentication	The IMPULSE system shall issue a challenge to verify that the user who is trying to authenticate is the owner of the VC	Must do	ALiCE, GRAD (UI)
FR-10	Authentication	The IMPULSE system shall check against the blockchain that the user's VC has not been tampered with	Must do	GRAD
FR-11	Authentication	The IMPULSE system (i.e., enterprise service) shall send a presentation request to the PA in charge of the requested online service	Must do	GRAD
FR-12	Usability Transparency Regulatory compliance	The IMPULSE system should inform the user about the status of the registration (onboarding) process	Must do	GRAD
FR-13	Usability Transparency Regulatory compliance	The IMPULSE system should inform the user about the status of the authentication process	Must do	GRAD
FR-14	Security	The IMPULSE system shall allow users to control their data in a self-sovereign manner	Should do	ICERT
FR-15	Security	The IMPULSE system shall protect identity information (e.g., ID document, facial, gender, location) that are most critical	Should do	ICERT
FR-16	Transparency Regulatory compliance	The IMPULSE system should allow the user to consult and request the deletion of their off-chain data	Should do	PA, GRAD
FR-17	Authentication Usability Transparency Effectiveness and reliability	The IMPULSE system should identify the reasons for failure of the authentication process and communicate them to the user.	Should do	GRAD
FR-18	Management of VCs	The IMPULSE 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	GRAD
FR-19	Authentication Face verification	The IMPULSE system shall match the user's face photo (selfie) to an existing VC stored in the device	Could do	GRAD

2.3.2 Non-functional ASRs (quality attributes)

The table below 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 (based on the requirements specification V1 D2.2).

Req. ID	Categories	Description	Testable / Verifiable	Priority	Involved partner(s)
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)	Y	Must do	ALiCE
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	Y	Must do	ALiCE
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	N	Must do	TREE
QA-04	Data protection Regulatory compliance Security	The public key should be stored in BC and anyway it must never be possible to trace back from the public to the private key	Y	Must do	ICERT, CEL
QA-05	Data protection and security	The system should prevent unauthorized third parties from accessing any user's personal data	N	Should do	GRAD
QA-06	Data protection and security	Biometrics and other personal identity data should be encrypted	N	Should do	ALiCE, GRAD
QA-07	Face verification Usability	The system should be able to recognize faces captured from images with different resolutions and illumination	N	Should do	ALiCE

Req. ID	Categories	Description	Testable / Verifiable	Priority	Involved partner(s)
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	N	Should do	GRAD
QA-09	Onboarding Usability Transparency	The system should provide simple and well-guided user actions when collecting image samples for face recognition	N	Should do	ALiCE
QA-10	Authentication Usability	The system should reduce cognitive burden (remembering many user accounts and passwords) for users.	N	Should do	GRAD
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	Y	Should do	ALiCE
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)	Y	Should do	ALiCE
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	Y	Should do	TREE
QA-14	Document verification Effectiveness and reliability	False Acceptance Rate (FAR) <= 1%: Out of 100 identity card or passport validation 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)	Y	Should do	TREE
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).	Y	Should do	CEL, ICERT
QA-16	Data protection Regulatory compliance Usability Transparency	The system should provide informed consent in a legal language and accessible with dedicated icons.	Y	Should do	CEL, ICERT
QA-17	Security Transparency	The system should indicate users where their personal data is stored.	Y	Should do	CEL, ICERT
QA-18	Portability and availability	The system should allow to authenticate users at any place and anytime	N	Won't do[3]	ALL

[3] The pilots will be conducted in a controlled environment and the testing of cross-border services is not part of the case study design of the IMPULSE project.

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 4 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.

On another hand, 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.

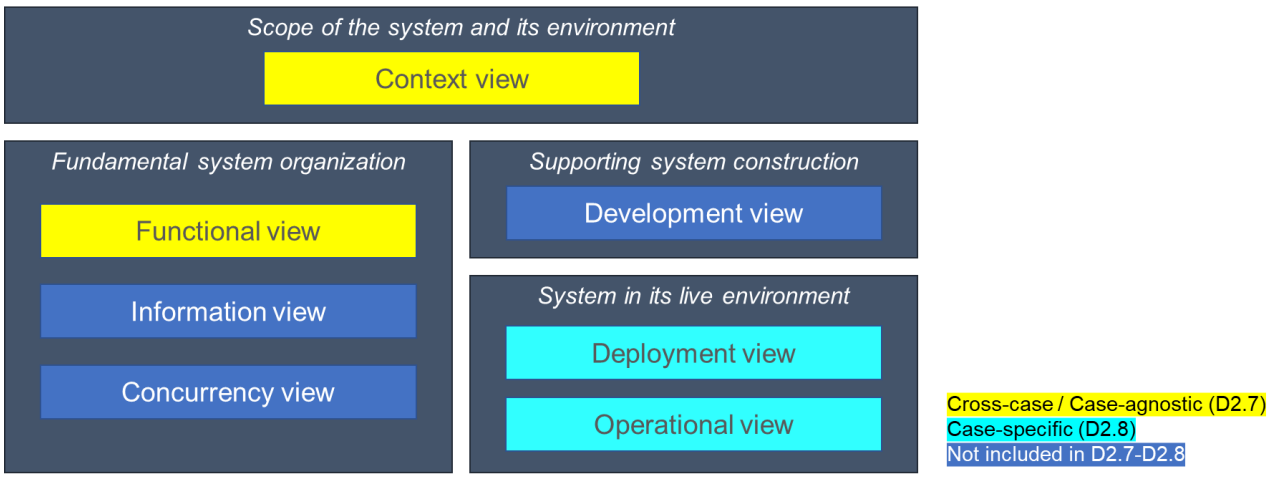


Figure 4: Architectural views covered in the specification deliverables of IMPULSE WP2 (D2.7-D2.8)

3.1 Main design decisions

These are key decisions consciously taken by the project partners (while discussing the options to address or implement the ASRs), which can have a significant impact or influence over the design of the software architecture. Design decisions emerge as a *response* of the technical team to solve specific ASRs or project constraints. In other words, a design decision differs from a software requirement or project constraint, because (1) it is not always requested by any specific stakeholder group or end-users, and/or (2) it is generally one of multiple other alternatives that the development team can choose from. Consequently, design decisions are often negotiable among project stakeholders and have "tangible" or measurable trade-offs (both positive and/or negative), which can be observed for example, in between the first and second piloting rounds of IMPULSE.

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 (+). 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 verifiable authorization (i.e., permission to write in the EBSI blockchain) are sent via email	DD-01	End user requires an email account and client, increased time during the registration / onboarding, waiting for the email notification (-).
DD-06	A list of VC, 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 (-).

Decision ID	Brief description and rationale	ASR or constraint from which this decision originates (if applicable)	Possible risks or trade-offs
DD-07	The app uses the language configured as primary in the smartphone. If translations are not available for this language, English is used by default.	QA-04	Easier setup (+). Less configurable (-).
DD-08	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 (-).

3.2 Context view

The purpose of the context view is to show the boundaries between the IMPULSE e-ID solution and other external software systems (i.e., managed and/or operated by third parties) to which it is integrated. In this view, the e-ID system under consideration is shown as a "black box", since the focus is on delimiting the scope of what is covered (or not) under the context of the project, as well as the interactions with other human actors (i.e., individuals and organizations) or systems in the surrounding environment. Figure 5 shows the context view of the IMPULSE e-ID solution.

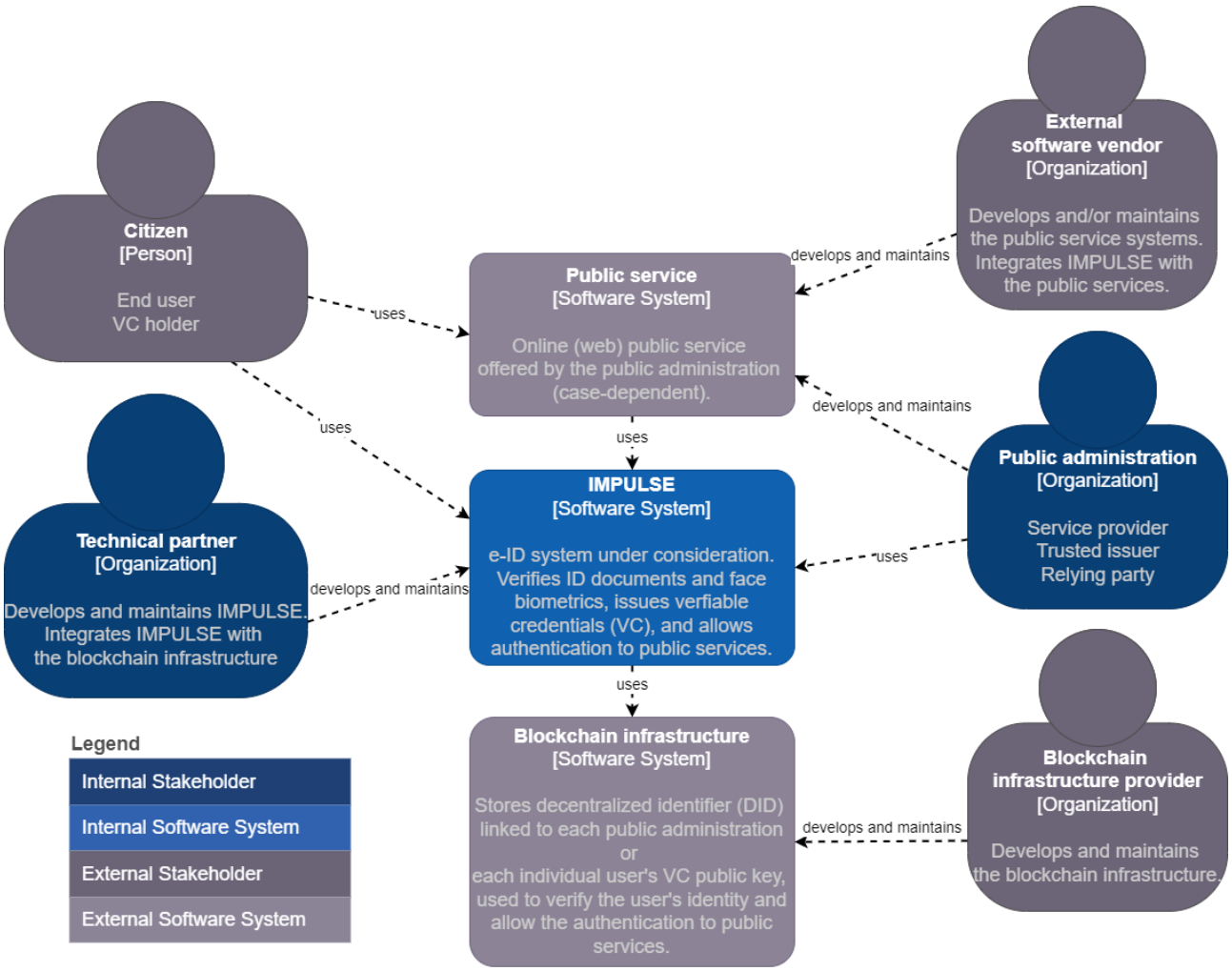


Figure 5: Context view of IMPULSE

3.3 Element catalogue

The element catalogue contains a list of the main blocks or functional elements of the IMPULSE e-ID solution, as well as any external systems to which it is integrated. The term "functional elements" refers to the logical units that allow the distribution of responsibilities (established in the functional ASRs) across different parts of the software system. In the architectural design, the functional elements can be represented at different levels of abstraction:

- Container: Separately deployable/runnable thing or runtime environment, typically (but not always) running in its own process space. It can fully or partially operate as a standalone part (can be "plugged in and out" of the software solution). Shown in Figure 6.
- Component: Grouping of related/interdependent functionalities, which have been encapsulated behind a well-defined interface
- Code (not included in the scope of the architecture specification deliverables V1-V2, D2.7-D2.8)

The table below lists the containers of IMPULSE with a single numeral using bold and underlined font. The components inside each container are listed with fractional/two-digit numbers and regular font.

Table 7: Catalogue of functional elements of the IMPULSE e-ID solution

No	Container Component	Type	Description / Functionality	Base technologies / Related projects	Provider / Owner
1	**Mobile (end user) app**	Internal, application container	Provides an interface for end users to interact with the IMPULSE e-ID solution through their mobile device	Android	GRAD
1.1	User wallet	Internal, module component	Module within the mobile (end user) app that stores and provides an interface to make use of the cryptographic material needed to interact in the SSI environment (DIDs, key pairs, VCs, VPs).	Android port created by GRAD of an open-source wallet called SSI Kit	GRAD
1.2	Biometric recognition module	Internal, module component	Selfie vs. Selfie verification: Module within the mobile (end user) app that analyses the selfie indicating whether it is a bona fide presentation and extracts the facial biometric profile to be stored locally in the end-user device. This module also enables comparison between two facial biometric profiles allowing user authentication. This process happens after the server side (i.e., biometric service) user registration on the platform.	Android, TensorFlow, JNI	AliCE
1.3	User interface	Internal, interface component	Interface used by end users to perform the needed operations in the IMPULSE e-ID solution.	Android	GRAD
2	**Enterprise service**	Internal, subsystem	Provides an interface for PAs to interact with the IMPULSE e-ID solution	Spring	GRAD
2.1	Enterprise wallet	Internal, 3rd party, module component	Module within the Enterprise Service that stores and provides an interface to make use of the cryptographic material needed to interact in the SSI environment (DIDs, key pairs, VCs, VPs).	SSI Kit	GRAD/ICERT[4]
2.2	Operator dashboard	Internal, interface component	Provides an interface for PAs' operators to manually approve or reject the onboardings to comply with eIDAS 2.0, since the biometric/document verification services might not provide enough accuracy.	Thymeleaf	GRAD

[4] The Enterprise Wallet component in IMPULSE makes use of the SSI Kit (https://github.com/walt-id/waltid-ssikit) libraries. However, these libraries lacked functionality needed in IMPULSE (e.g., ESSIF Onboarding Service). This missing functionality has been developed by GRAD, and it can therefore be considered a provider for this component. ICERT also researched about the SSI Kit, tested the Enterprise Wallet and actively participated in the discussions regarding this component.

3	**Biometric service**	Internal, subsystem container	Selfie vs. ID document verification: This service is invoked by the enterprise service to perform the biometric verification that matches both faces, selfie and ID document. It is available via API REST and it is intended to check first whether the user's selfie is a bona fide presentation and second, whether the selfie belongs to the same identity as the ID document. This identity verification happens when registering as a user on the platform.	Python, TensorFlow	ALiCE
4	**Document verification service**	Internal, subsystem container	This service is invoked by the enterprise service for validating the identity documents uploaded by the users	Optical Character Recognition (OCR), AI, SERIF (fraud detection service)	TREE
4.1	Photos quality check	Internal, service component	This service checks the quality of the ID document photos (brightness and sharpness levels, characters visibility, etc.). In the case of a bad quality, the system needs to ask the end-user for a new photo.	Image processing, OCR	TREE
4.2	MRZ Reader	Internal, service component	This service reads the machine-readable zone (MRZ) of the identity document, checks that it is valid and returns field information to be stored in the VC	OCR, MRZ Validation	TREE
4.3	Copy-move tampering detector	Internal, service component	This service gives an estimation of the fact that some parts of the identity document image have been copied and pasted within the same image	Scale-Invariant Feature Transform (SIFT), AI, Machine Learning (ML), Clustering	TREE
4.4	Imitation forgery detector	Internal, service component	This service gives an estimation of the fact that some characters of the document have been manually introduced, and not officially printed by the authorities	OCR, Feature Engineering, AI, ML, One-class Classification	TREE
5	**Remote qseal service**	Internal, subsystem container	This remote service is requested by the ESSIF implementation to be technically aligned with eIDAS references. The system signs a (JSON) VC by creating a valid eIDAS signature in JWT format within the Proof attribute. The system is not connected to an eIDAS node.	JavaEE service, JWT, eIDAS algo	ICERT
6	**Informed Consent Service**	Internal, service component	This service allows the user to give the consent of sharing personal information inside the Impulse solution. This consent is stored in a public blockchain using smart contracts.	JavaScript	CEL

3.4 Functional view – Container diagram

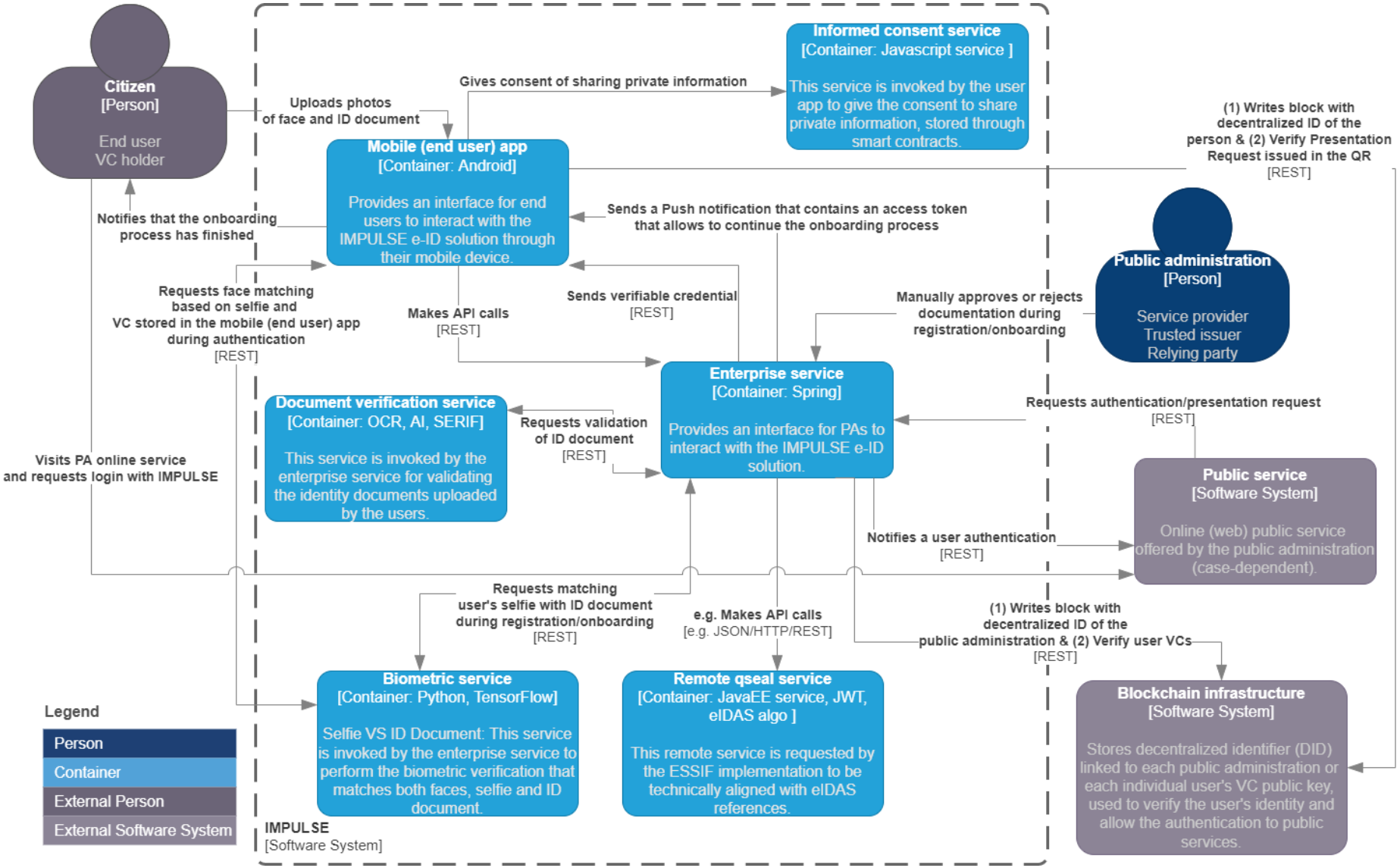


Figure 6: Highest-level blocks of standalone deployable or runnable functionality (i.e., containers) in the IMPULSE e-ID solution

4 Conclusions

This deliverable aimed to provide a view of the high-level software architecture design of IMPULSE and answer the following research questions and sub-questions.

- How does a new e-ID solution based on the vision and stack of disruptive technologies of IMPULSE work?
    - Who are the main actors that interact directly or indirectly with the e-ID solution?
    - What are the main features and use cases of the e-ID solution?
    - What is the scope or boundary between the e-ID solution and other software systems or platforms?
    - How are the functional responsibilities of the e-ID solution distributed among different components?
- 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?

IMPULSE has multiple stakeholders, such as users/citizens, public administrators and technical partners. Each stakeholder have different needs and concerns that influence the requirements of the architecture. Based on these existing literature, technology, and stakeholder concerns, functional and non-functional ASRs were collected and divided into three categories by their priority using the MoSCoW method. The priorities are tied to the end-user pilots:

- **Must do** functionalities have to be implemented before 1st round of pilots
- **Should do** functionalities need be implemented before 1st or 2nd round of pilots
- **Could do** functionalities may be done before 2nd round of pilots.

Two thirds of the identified functional requirements belong to “must do” category while only a third of non-functional requirements have the same priority. This is due to functional requirements being important to get a working product while the non-functional requirements are quality of life improvements on a working product. Most non-functional requirements are prioritized as “should do” and are meant to be completed before the 2nd round of pilots.

The collected requirements were used as a basis for the architectural design of IMPULSE. The results of the architectural design process described in Chapter 3 of this deliverable were presented to the rest of IMPULSE partners in a workshop on March 17th, 2022, during a face-to-face meeting of the Consortium. During this same session, the technical partners also held a short demonstration of the process to deploy or instantiate the IMPULSE e-ID solution to each of the PA’s local environments.

The high-level architecture, which is based on a client-side / end-user mobile application app and an enterprise service deployed to the PA’s local environment, allows for a relatively straightforward and simple instantiation process.

Some of the key design decisions related to critical aspects of the software architecture, such as the adoption of the EBSI/ESSIF as blockchain network and governance framework, respectively (DD-01), were adopted internally by the members of the Consortium after considering different options and under the recommendations of the EC for alignment with European initiatives. . This key design decisions might be perceived differently by other external stakeholder groups, such as service providers, citizens, or policymakers, who can influence the future adoption and overall viability of IMPULSE. Similarly, other key design decisions like the need for manual ID verification during the registration process (DD-02), the limited range of valid ID document types accepted by the e-ID solution (DD-03), and the asynchronous communication between the document verification and the enterprise service of IMPULSE (DD-04) will almost certainly have an impact in the perceived usefulness and usability of the e-ID solution during the pilot experiments. Nevertheless, the consortium made these decisions considering the best options for the IMPULSE solution development and for expecting the user's acceptance

In general, the PAs expressed they had reached a better understanding of the scope, functionalities, and dependencies of the e-ID solution after the presentation of the architectural design and the live demonstration.

At the same time, the session also revealed the need to continue clarifying the goals, steps, and operational setup of the pilot case experiments.

Still some operations need to be more defined, but other tasks and deliverables of WP2 will continuously contribute to reduce these gaps between the design/development of the e-ID solution and the preparation of the local testing environments, e.g.:

- **T2.2/D2.5-2.6 Piloting roadmap V1-V2:** Defining the prerequisites and operational setup of the pilot experiments
- **T2.4/D2.9-2.10 Implementation of basic system V1-V2:** Performing the required modifications or adaptations of the e-ID solution, together with the necessary documentation and technical support, in order to enable a smooth integration of the e-ID solution into the PA's local service environments

The next iteration of this architecture specification deliverable (V2, D2.8) should also expand the architectural design and architectural evaluation of the pilot-specific aspects:

- **Architectural design:** Incorporating the deployment, integration, and operational views
- **Architectural evaluation:** Doing walkthroughs of the scenarios related to each pilot´s use case

Besides illustrating the design of the baseline software architecture and the pilot behaviour of the IMPULSE e-ID solution *as-is*, the architecture specification V2 (D2.8) must address other aspects related to its future governance and change management of the IMPULSE e-ID solution, in alignment with The Open Group Architecture Framework (TOGAF). In particular, at least the following aspects should be clarified:

- How to reduce dependencies on specific blocks or services provided by the Consortium partners, allowing for increased interoperability or compatibility with similar solutions offered by other companies
- How to enable the solution to be used with any blockchain technology that supports a Self-Sovereign Identity model
- How to agree and handle between the technical partners and the public administrations the processes related to automated event logging, remote monitoring and control, maintenance and support, migration, and continuous integration / continuous deployment pipeline

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.