Identity Management in PUbLic SErvices

Impulse

D2.2 IMPULSE requirements specification - V1

Lead Author: Nasren Azad (LUT)
Reviewers: Pedro López (GIJON), Georgi Simeonov (MOP)

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Delivery date:	09-09-2021
Version:	1.0
Total number of pages:	38
Keywords:	Requirements, case studies, co-creative design, piloting, software quality, usability, trusted access

Executive summary

The work package 2 (WP2) of IMPULSE explores the requirements for the onboarding and authentication processes of the electronic identification (e-ID) solution that will be pilot tested with users of six different cases. The goal is to know how trustworthy, usable, and inclusive the IMPULSE solution can be for citizens, in particular those that might face greater barriers for its adoption, such as elderly people and female users.

D2.2 follows the stakeholder analysis presented in D2.1. The focus of D2.2 is to identify a set of formal requirements for the IMPULSE solution. The requirements elicitation will be focused on the general, cross-case quality attributes of the system, particularly on the adaptations to the base platform components required to facilitate usability, user experience, and trust.

The deliverable is based on the following activities:

- Literature review and classification of general requirements, conducted from February to May 2021. The review comprised several topics, such as e-ID, regulations, GDPR, blockchain, artificial intelligence, as well as different methods and approaches to co-creative requirements elicitation.

- An online workshop session with two co-creation activities, namely card sorting and user stories. These methods helped to identify high-level goals for e-ID, validate and refine general requirements found from the literature review, and identify any missing or additional requirements for the IMPULSE e-ID solution.

Based on the activities listed above, the initial set of general requirements for IMPULSE was established. These requirements will be further refined in two iterations, which will be delivered in subsequent deliverables, D2.3 (V2) and D2.4 (V3).

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**	D2.2	**Title**	IMPULSE requirements specification – V1
Work package	**Number**	WP2	**Title**	Co-creative design and piloting
Task	**Number**	T2.2	**Title**	Co-creative requirements elicitation scheme and piloting roadmap

Date of delivery	**Contractual**	M07	**Actual**		M08
Status	version 1.0		☐Final version		
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)				
Dissemination level	☒Public ☐Confidential				

Authors (partners)	LUT			
Responsible author	**Name**	Nasren Azad		
	Partner	LUT	**E-mail**	nasren.azad@lut.fi

Summary (For dissemination)	WP2 explores the requirements for authentication and onboarding process of e-ID solution for users. The goal is to know how trustworthy, usable, and inclusive the IMPULSE solution can be for citizens, users, policymakers, and vulnerable groups of citizens. The aim of D2.2 is to identify a set of formal requirements for the IMPULSE solution. The requirements elicitation is focused on the quality attributes of the system, particularly on the adaptations to the base platform components required to facilitate usability, user experience, and trust. The deliverable is based on two major activities. The first activity was the literature review on e-ID, relevant legislation like GDPR, blockchain, AI, and co-creation methods and approaches, to identify general requirements for the future IMPULSE solution. Thereafter, a co-creative session with card sorting and user stories was conducted, to identify high-level goals for the future IMPULSE e-ID solution. The card storing helped validate and refine the general (cross-case) requirements identified in the literature. The user stories helped identify additional requirements for the IMPULSE e-ID solution.
Keywords	Requirements, case studies, co-creative design, piloting, software quality, usability, trusted access

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
26-07-2021	0.1	Nasren Azad (LUT)	First draft version
26-08-2021	0.2	Annika Wolff, Bilal Naqvi, José Camposano (LUT)	Internal LUT review
07-09-2021	1.0	Pedro López (GIJON), Georgi Simeonov (MOP)	IMPULSE review

List of figures

List of tables

Table of contents

Abbreviations and acronyms

AI: Artificial intelligence

ARH: City of Aarhus, Denmark

DoA: Description of action (IMPULSE project)

e-ID: Electronic identification

ERTZ: Basque Government – Security Department – Ertzaintza

GIJON: City of Gijón, Spain

IEC: International Electrotechnical Commission

ISO: International Organization for Standardization

MOP: Municipality of Peshtera, Bulgaria

UC/IC: Union of Italian Chambers of Commerce / InfoCamere

RVK: City of Reykjavik, Iceland

SO: Specific objective (IMPUSE DoA)

WP: Work package (IMPULSE DoA)

1   Introduction

This deliverable (D2.2) initiates the co-creation activities for work package 2 (WP2). This deliverable presents relevant details about 6 different case organizations participating in the WP2. This gives an overview on how the requirements extraction process will be done throughout the project. For the overall feedback of the IMPULSE solution, various aspects and viewpoints of stakeholders were considered.

There will be three versions of this requirement specification document. D2.2 is the first version (V1) of the requirements specification (technical and organisational). This is expected to contribute towards the launch of first prototype for IMPULSE in M15 (T2.4). The second version (V2) of the deliverable will focus on the adaptation of the general requirements into pilot specific requirements (D2.3). The final version of the deliverable will include the formal general requirements for IMPULSE solution (D2.4).

Overall, the focus during the project in general and the WP2 will be on the public services and identification process for diverse groups of stakeholders including citizens, public servants, technologists, policy makers and regulatory authorities, etc.

1.1   Objective of the deliverable

The objective of the deliverable D2.2 is to gather general requirements for the IMPULSE solution, which will be refined by taking into consideration the commonalities and differences observed across six pilot cases (ARH, ERTZ, GIJON, MOP, RVK, UC/IC). The refined set of requirements will be delivered to the technology partners, to provide essential input to guide the system design. Thereafter, the solution will be tested through the 6 case studies.

D2.2 presents the first set of IMPULSE requirements, which were mainly gathered through analysis of the existing literature. The requirements were later refined and validated by applying a co-creation approach. To achieve this goal, an online co-creation workshop was organized with the IMPULSE consortium partners. Moreover, additional requirements relevant to IMPULSE use cases, which could not be identified in the existing literature, were also identified and documented during the workshop.

D2.2 also forms the basis for adapting the general requirements into pilot specific requirements. Thus, the academic literature and the co-creation activities will support the future workshops and pilot activities for the IMPULSE solution.

D2.2 aligns with the following goals of the proposal:

Goal 1: Specify the requirements, acceptance, and impact on the use of e-ID technology from regulatory, technical, operational, and societal standpoints through the engagement of stakeholders in a co-creative demand-driven research process, including pilots in 5 different countries.

- SO1.1 Evaluate operational aspects, acceptance, usability and inclusion, security, and privacy protection (in line with goals 2 and 3) in real-life public services through 6 different case studies to address the identified critical challenges. KPI: Acceptance, accessibility, and usability rates (>70%).

- SO1.2 Co-create a holistic and sustainable blockchain-based e-ID solution responding to the needs of multidisciplinary stakeholders based on the status of research and technical standards through an agile approach for an efficient specification, implementation, and validation. KPI: No. stakeholders involved (>100) and detailed requisites (D2.2).

The main contributions of D2.2 are:

- Performing literature review on e-ID, co-creation, user-centered design, participatory design, design science and e-ID regulations.
- Identifying the initial cohorts for conducting the co-creation activities
- Defining the methodological approach to co-creation
- Conducting a co-creation workshop with project partners, case owners, and researchers, to refine the general requirements from literature.
- Communicating and documenting the general requirements for the different cases and across cases.
- Building a better, common understanding of the workshops and pilots among the case owners and partners of the project.

1.2   Timeline

D2.2 corresponds to the first stage of the co-creative requirements elicitation process, comprising different research activities that took place during the initial seven months of the project, starting from February 2021 until August 2021. These research activities began with a literature review, which allowed the team to review and discuss the general requirements found from the literature. This review was followed by an online co-creation workshop, which took place on June 23rd, 2021. After getting and collecting all the inputs from the workshop participants, the findings were analysed and documented in this deliverable.

2   Requirements elicitation process

The deliverable has been prepared using the inputs of four activities: 1) literature review 2) analysis of the case description 3) analysis of the project proposal 4) co-creation workshop. These activities are shown in Figure 1. Next, we describe these activities into more detail.
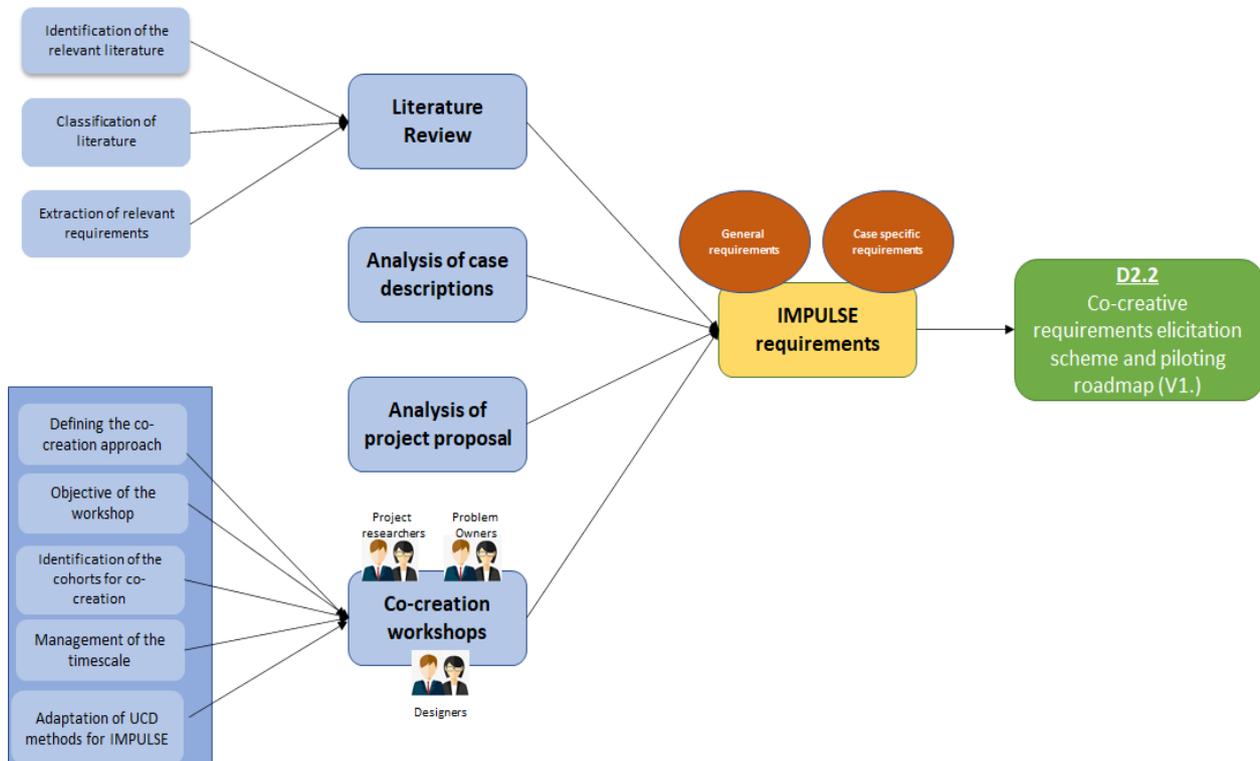
Figure 1: Research methodology for D2.2

2.1   Literature review

2.1.1   Identifying the relevant literature

We conducted a literature review to identify the most essential requirements for the IMPULSE solution. To identify the relevant literature, a search was performed on Google Scholar using the keywords taken from the DoA. The following keywords were used to –perform the search on Google Scholar.

- 'e-ID' AND 'user requirements'
- 'Electronic identity' AND 'user requirements'
- 'Blockchain' AND 'e-ID' AND 'user requirements'
- 'Blockchain' AND 'electronic identity' AND 'user requirements'
- 'Artificial Intelligence' AND 'electronic identity' AND 'user requirements'
- 'AI' AND 'electronic identity' AND 'user requirements'

The search results were then subjected to filtering and screening, by reading first the titles and then the abstracts of the research papers. Only the papers presenting user requirements related to electronic identity solution were considered for further analysis.

2.1.2   Classification and synthesis of the literature

Based on the search results, the identified literature with research papers on user requirements for e-ID, AI for e-ID, and blockchain for e-ID, were classified while considering the definitions and terminologies identified in the ISO/IEC 25010 standard, which lists some of the main quality characteristics that must be considered during the evaluation of a software product. The three major interconnected themes identified after the classification of the literature are:

To classify the literature, we considered research papers on e-ID, user requirement on e-ID, user requirements and Blockchain, Artificial intelligence (AI) with e-ID, GDPR issues and Blockchain, e-IDAS. Based on the clustering of papers, three major interconnected themes were identified. The themes are:

- Technical issues
- Regulatory issues
- Issues related to user acceptance

2.1.2.1   Technical issues

The literature classified under the technical issues theme is centred around how to improve e-ID systems to make them more secure, which is one of the main quality characteristics described by ISO-25000. Topics commonly discussed in prior research include biometrics, authentication processes, and decentralized identity systems. Recent research has also discussed the use of blockchain, which is one of the key technologies of the IMPULSE solution.

Blockchain literature can be broadly categorized into two categories: 1) moving existing certificates to "on chain" and 2) building self-sovereign identity management systems using blockchain (Bazarhanova et al., 2019). The logic behind using blockchain for e-ID solutions is to provide more control to the data owners. In blockchain based e-ID solutions, there is no central authority because such solutions run in a peer-to-peer network. In blockchain-based e-ID systems, personal information can only be revealed with explicit consent.

2.1.2.2   Regulatory issues

This stream of literature describes legal and regulatory analysis of the e-ID solutions. In particular, e-IDAS, GDPR and country specific regulations are discussed. The e-ID solutions should follow the local and global regulatory requirements for user uptake (Bazarhanova et al., 2019). New challenges emerge in terms of GDPR requirements when using blockchain. As blockchain data cannot be deleted, it is a challenge to meet the GDPR requirement of "right to be forgotten" (Haque et al., 2021). Furthermore, it is difficult to identify the data controller (a GDPR requirement) because the blockchain is maintained by many miners.

2.1.2.3   Issues related to user acceptance

The final stream of literature discusses issues related to user acceptance. Lirginlal and Phelps (2012) view e-ID as a sociotechnical system and analyse the implementation of digital identity in Qatar. They identified social, economic, technical, and legal barriers. Hedström et al. (2015) also portray e-ID as a sociotechnical system and use actor network theory to identify the actors and motives in e-ID implementations. They found that different actors in the network possess different ideas about e-ID. For example, the information security manager thought that e-ID is necessary to be implemented for improving security for the patient data. However, the nurses thought that the e-ID card was a constraining commodity.

Tsap et al. (2019) conducted a literature review to identify the factors that impact user acceptance. They identified 11 major factors that affect e-ID acceptance. The factors are (1) complexity; (2) ease of use; (3)

functionality; (4) awareness; (5) trust; (6) privacy concerns; (7) security; (8) control and empowerment; (9) transparency; (10) path dependency and (11) cultural and historical factors.

Some of the user-related aspects listed above, such as control and empowerment, transparency, and trust, can be ensured in blockchain-based self-sovereign identity management systems. Also, these aspects are related to the characteristics of usability and security from the ISO/IEC 25010 product quality model.

2.1.3   Extracting relevant requirements

After filtering and screening the search results, we read the full text of the selected articles and extracted the relevant user requirements. During the extraction process, minor adjustments were done to the original wording of the requirements, to match better with the specifications of IMPULSE. The primary author of this deliverable was responsible for the initial extraction of the requirements from the literature and identified an initial list of 37 requirements. After careful analysis, removing redundant requirements, and merging the similar ones, 35 requirements were retained. Thereafter, another researcher revised the requirements and assessed their relevancy to IMPULSE. At this stage, a few requirements were deemed not relevant to IMPULSE and were removed from the list. The wordings of the requirements were also slightly adjusted to fit with IMPULSE at this stage. At the end, we ended up with 26 requirements for further validation. Next section presents these 26 requirements.

2.1.4   Findings from the literature review

The requirements extracted from the literature review were categorized based on the product quality characteristics identified by ISO/IEC 25010 quality model, which explains about the product quality and how the system is evaluated. The ISO/IEC 25010 includes characteristics such as security, compatibility, portability, usability, among others. This model identifies what quality characteristics should be considered while evaluating the properties of a software product.

In line with the definitions of various characteristics identified by the ISO/IEC 25010 product quality model, the identified IMPULSE requirements can be categorized into the following different categories: Security, compatibility, portability, and usability. Moreover, due to the regulatory requirements in IMPULSE, a few requirements can be categorized under the 'consent management' category, even though consent management is not listed among the characteristics of ISO/IEC 25010 quality model. The final categories of the requirements are shown in Figure 2. Next, we describe each of these categories into more detail.
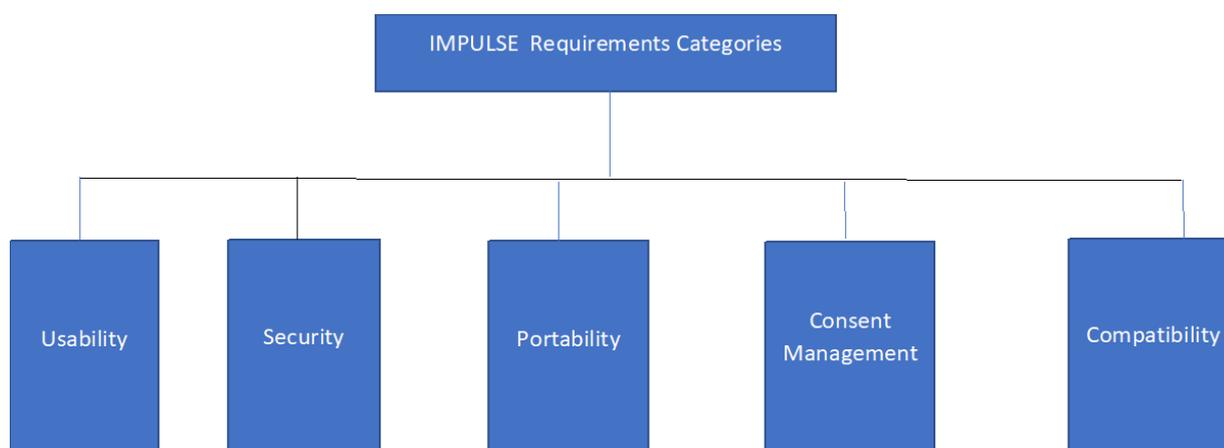

Figure 2: Requirements classification from literature review

2.1.4.1   Usability

Usability refers to 'the degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use' (ISO-25000). The general requirements identified from scientific literature and related to usability are:

1. The system should provide seamless identity management for users through a good design interface (Dhamija & Dusseault, 2008).
2. The system should be easy to download, install, and configure (Dhamija & Dusseault 2008).
3. The system should enable time saving features such as automated form filling and single sign-on across the online public services that the user wants to access (Dhamija & Dusseault, 2008).
4. The system should provide the option to choose a particular identity if the user has multiple identities stored on his or her device when logging to a public service. (Alpar et al., 2011; Oruaas & Willemson, 2020).
5. The system should simplify the process of updating the user's verifiable credentials (e.g., address changes) (Alpar et al., 2011).
6. The system should be able to recognize faces captured from images with different resolutions and illumination. (Kamgar et al., 2011).
7. The system should reduce cognitive burden (remembering many user accounts and passwords) for users (Dhamija & Dusseault 2008).
8. The system should identify the reasons for failure of the authentication process and communicate them to the user (Wang et al., 2014).
9. The system should provide simple and well guided user actions when collecting image samples for face recognition (Tan et al., 2010; Wong et al., 2011).

2.1.4.2   Security

Security refers to the 'degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their type and levels of authorization' (ISO-25000). The general requirements related to security that were identified from scientific literature are:

1. The system should maintain users' privacy by improving protection of the users' personal data (Dhamija & Dusseault, 2008; Zirjawi et al., 2015).
2. The system should indicate users where their personal data is stored (Stuedi et al., 2010)
3. The system should keep users' location confidential (Zirjawi et al., 2015).
4. The system should allow users to control the use of their data in a self-sovereign manner (Dunphy and Petitcolas 2018).
5. The system should allow users to control the information released from the identity provider (IdP) (Alpar et al., 2011).
6. The system should allow smart contracts between the citizen and the service provider to establish on how to process the data (Bazarhanova et al., 2019).
7. The system should allow removing users' off-chain data if they want (Wirth et al., 2018).
8. The system should use an off-chain solution if blockchain is used for data storage (Hepp et al., 2018).
9. The system should consider anonymity and pseudo anonymity to be implemented whenever possible (Alper et al., 2011; Bazarhavona & Smolander, 2020).
10. The system should protect identity information (e.g., fingerprint, facial), which are most critical (Bojinov et al., 2014).
11. The system should be designed in such a way that additional software packages are not needed to protect identity. Users do not want to purchase or use additional software packages to protect identities (Dhamija & Dusseault, 2008).

2.1.4.3   Portability

Portability refers to 'the degree of effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment to another' (ISO-25000). The general requirements related to portability that were identified from scientific literature are:

1. The system should allow users to create, manage, and use his or her identity independently of his or her location and device in use (Alper et al., 2011).

2.1.4.4   Consent management

We define consent management as the process that allows a product or service to meet regulatory requirements (e.g., GDPR) by obtaining user consent. The general requirements related to consent management that were identified from scientific literature are:

1. The system should allow users to know how their data would be used and if it is safe from unauthorized access and processing (Wirth et al., 2018).
2. The system should provide short and clear messages and warnings when asking for consent (Dhamija & Dusseault, 2008).
3. The system should reveal any personal identifiable information of users only with explicit consent (Bazarhanova et al., 2019; Dhamija & Dusseault, 2008).

2.1.4.5   Compatibility

Compatibility refers to the 'degree to which a product, system or component can exchange information with other products, systems or components, and/or perform its required functions while sharing the same hardware or software environment' (ISO-25000).

1. The system should be interoperable with the legacy e-ID schemes to ensure user uptake (Bazarhanova et al., 2019).
2. The system should allow reuse of verifiable credentials in the ecosystem (Bazarhanova et al., 2019).

2.2   Analysis of the case descriptions

The IMPULSE project considers six unique use cases (ARH, ERTZ, GIJON, MOP, RVK, UC/IC). During the initial seven months of the project, several meetings were conducted with the case owners to understand their case context and scope.

Since the start of the project, some of the pilot case descriptions have been changed and modified gradually, based on discussions about the need for adaptation to the technical constraints, legal issues, or other limitations of the cases. However, it was found that some requirements are common to all cases. These requirements were also considered in the list of requirements presented in this D2.2. The cross-case requirements identified from the case descriptions are:

Usability

1. The system should allow all case owners to have a solution which will help the users and citizens to perform authentication process safely, effectively, and efficiently while enjoying experience of the solution for services.

2. The facial recognition system will be applied for all cases where sensitive data will be omitted.

Security

1. The system should provide security for data protection so that imposters cannot access it.

Portability

1. The verification system should be able to authenticate users in any place and anytime.

2.3   Analysis of the project proposal

The information extracted from the proposal are as follows:

4. The system should have access to specific services which is personal and non-transferable.
5. The system should provide a secure and trustful identification for citizens.
6. The system should provide an identity which allows citizens, businesses, and administrations to be distinguished from each other.
7. The system should provide an e-ID solution that can guarantee the unambiguous identification of a person and make it possible to get the service delivered to the person who is really entitled to it [EC_e-ID; eSSIF].
8. The system should be able to provide secure and privacy-preserving e-ID solution.
9. The system should provide public administrations a solution that resolves overlapping (or even contradictory) versions of the same digital identity.

IMPULSE will transform the mainstream discourse on digital identity by drawing up a user-centric multi-stage method of multidisciplinary evaluation of e-ID management that combines the bottom-up approach of co-creation with the need for a universal vision of digital identity ethics in providing public services.

2.4   Co-creation workshop

Co-creation workshops seek to involve different participants, such as end users, researchers, developers, and legal experts, to work together to find a solution for a specific problem. In IMPULSE project, a co-creation workshop was conducted to refine and validate the requirements identified after the literature review, as well as to identify additional requirements for the IMPULSE solution. The insightful outcomes from the co-creation workshop will also be helpful for planning future co-creation workshops for requirement elicitation.

2.4.1   Defining and adapting the co-creation approach for IMPULSE

Two different co-creation methods were used in the co-creation workshop: (1) card sorting, and (2) user stories. Each of these methods are discussed in the following sections.

2.4.1.1   Card sorting

Card sorting is a method used to classify and evaluate a series of cards, which are labelled with a piece of content and functionality for a group of participants (Spencer et al., 2004). In the card sorting session, participants can write and organize topics and categorise them in a way that makes sense for the objective(s) of the workshop. To conduct a card sorting session, there can be actual cards on pieces of paper or there could be several online card sorting tools to use.

There are two ways card sorting can be done:

- Closed card sorting
- Open card sorting

Closed card sorting is defined as a methodology in which grouping is defined by the researchers and the subject is putting object cards into a defined group (Hannah, 2008). Open card sorting is defined as a methodology in which subjects can determine their own grouping by first sorting the cards and then labelling the resulting piles (Hannah, 2008). Participants are asked to organize topics from content which makes sense to them and then name each group they have created in a way which describes the content accurately.

The open card sorting methodology was used for the co-creation workshop described in this deliverable. The reason for using card sorting was to cluster, validate, and refine general (cross-case) requirements found in the literature. In the co-creation workshop section, it will be discussed in further detail.

2.4.1.2 User stories

A user story is a general explanation of an application feature, which has been written from the perspective of the end user. User stories help to elicit software system requirements and are widely used in agile development (Lucassen et al., 2015). User stories put the end users at the centre of discussion and use non-technical language to provide feature description that can be used by the development team. When a development team reads a user story, it gives knowledge about what solution the development teams are making, why are they making the solution, and what value will it create for the user (Lucassen et al., 2015). User stories have the following format:

"*As a* (*type role*), *I want* (*some goal*) *so that* (*you can be benefited*)"

2.4.2 Objectives of the co-creation workshop

The objectives of the co-creation session are (1) to identify high-level goals for the future IMPULSE e-ID solution, (2) to validate and refine general (cross-case) requirements found in the literature through card sorting, and (3) to identify missing or additional requirements for the IMPULSE e-ID solution through user stories.

2.4.3 Identifying the cohorts of the co-creation workshop

The goal of the co-creation workshop was to involve different stakeholders, including technologists, co-creation experts, problem owners (i.e., representatives from public administrations) and citizens. Given the complexity of engaging citizens in an early project stage when no prototype exists, the lack of common procedures for ensuring ethical and legal compliance, and the focus of the project on new technologies that are difficult to describe in abstract form, it was decided to include only the members of the IMPULSE Consortium acting in dual role (i.e., as partners and as citizens) during this phase of the co-creation process. In this way, they have already acquired enough understanding by engaging with IMPULSE and the supporting technologies. However, future iterations of this deliverable (D2.3 and D2.4) will include non-"partner/citizens". This creates some limitations on the preliminary findings of D2.2, but since there are two further iterations of this requirements document and we will ultimately have a prototype to serve as a basis for eliciting the requirements, we will still gain citizen input to this process and future workshops will take place with citizens participation from six municipalities.

To recruit the participants for the first co-creation workshop, an invitation was sent via email. It was requested to the case owners to ensure the participation of at least one representative of each public administration in the workshop. The workshop had 18 participants in total, including the hosts. The participants involved in the co-creation process were researchers (as facilitators), technical experts, legal experts, and case owners.

2.4.4 Workshop activities

The workshop was conducted online via Microsoft Teams because of the COVID-19 pandemic and related logistical challenges to gather all participants at the same physical location. There were 3 tasks during the co-creation workshop:

1. Identifying high-level goals for the IMPULSE e-ID solution

2. Card sorting exercise
3. Creating user stories to identify additional requirements

Due to the co-creative nature of the tasks, the online collaboration tool Miro was used during the workshop. The facilitators gave a brief introduction and tutorial of this tool at the beginning of the workshop. Afterwards, the participants were given instructions on how to complete each task in Miro board. They were divided into three groups (yellow, pink, and blue) and assigned to three separate breakout rooms in Teams, in order to perform the tasks.

Task 1: Identifying high level goals

The first task for the workshop participants was aimed at identifying high level goals for the IMPULSE e-ID solution. This task was divided into two sub-Tasks, Task 1.1, and Task 1.2:
- Task 1.1 consisted in brainstorming in groups and identifying the high-level goals. Some guiding questions to be considered in the groups were: "Why do you need IMPULSE solution?" and "What do you expect from IMPULSE solution?" The participants were also provided with some examples of high-level goals to further clarify this task.
- Task 1.2 consisted in creating a unified list of high-level goals, based on the individual outcomes of each group after the prior task and the discussion among all participants of the workshop.

Task 1.1 started in the breakout rooms of each team, where the participants discussed with their peers and wrote down the high-level goals on sticky notes. After all groups completed this task, they were recalled to the main room to proceed with the next sub-task. Figure 3 below shows the online collaboration workspace that was designed for Task 1.1.
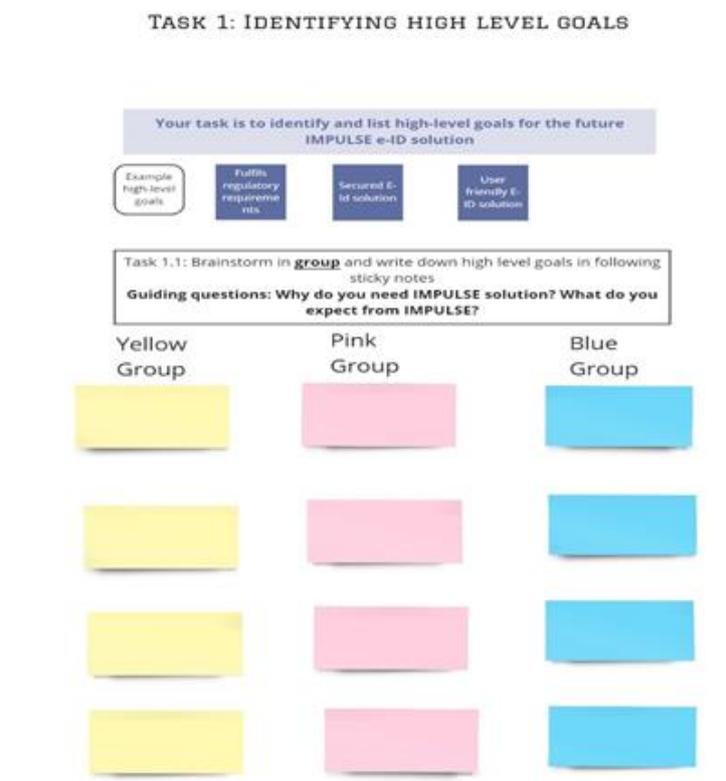

Figure 3: Workshop task 1.1 – Identifying the high-level goals for the IMPULSE e-ID solution

For task 1.2, all groups returned to the main room and merged their contributions into a single list of high-level goals. The participants dragged and dropped sticky notes containing similar high-level goals and clustered them. Afterwards, the workshop facilitators discussed with the participants and agreed to assign a name to each cluster. The outcomes of clustering are shown in Figure 4.
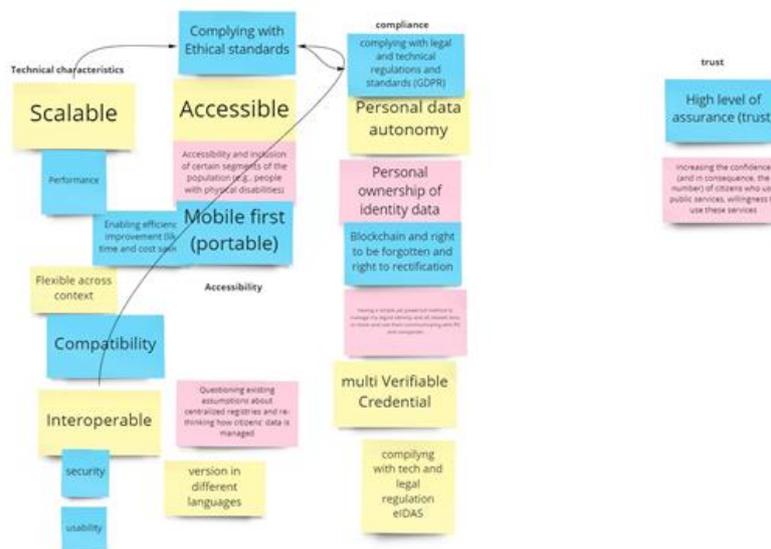
Figure 4: Workshop task 1.2 – Clustering high-level goals

Task 2: Card sorting exercise

The second task for the participants was aimed at validating and refining the general (cross-case) requirements found in the literature, by means of a card-sorting exercise. Each group was assigned a set of requirements identified from the literature and asked to relate those requirements to any of the high-level goals identified during the previous task. All the requirements that could be related with at least one of the high-level goals were the ones validated as highly relevant or having a direct contribution to the desired IMPULSE solution, Requirements that could not be related to any high-level goals were considered less relevant or not contributing directly to the main goals of IMPULSE. An adapted card-sorting technique was used due to online nature of the event.

Figure 5 below presents the outline of the task. The requirements were presented in the left column and the high-level goals were presented in the subsequent columns towards the right-hand side. Each group was assigned 8-9 requirements. The participants were asked to put a "thumbs up" under the column representing each high-level goal or goals (if any) that they considered were directly related to the requirement written in the first column of the table.

Figure 5: Workshop task 2 – Card sorting to validate the requirements from scientific literature

Task 3: Creating user stories

The task was aimed at identifying missing or additional requirements for the IMPULSE e-ID solution by creating user stories. User story is a technique that help gather requirements from the perspective of the target user groups of the IMPULSE solution. User stories are generally phrased with the template format below:

As a (you need to give a role) I want (there should be a goal) so that (I can get benefit).

Figure 6 below shows the online collaboration canvas that was created for task 3 of the workshop.

Figure 6: Workshop task 3 – Creating user stories to identify additional requirements

2.4.5   Findings of the workshop

This section describes the outcomes and findings of the three tasks of the co-creation workshop.

Task 1: Identifying the high-level goals for IMPULSE e-ID solution

The three groups were labelled as yellow, pink, and blue. Each of them discussed and brainstormed with their group members and identified various high-level goals, which are listed below:

High-level goals for yellow group
- Scalable
- Accessible
- Personal data autonomy
- Flexible across context
- Interoperable
- Multi variable credential
- Version in different language
- Complying with tech and legal regulations e-IDAS

High-level goals for pink group
- Accessibility and inclusion of certain segments of the population (e.g.: People with physical disabilities)
- Personal ownership of identity data
- Increasing the confidence of citizens who use public services, willingness to use these services
- Having a simple yet powerful method to manage my digital identity and all related data, to share and use them in communication with PA and other companies.
- Questioning existing assumptions about centralized registries and rethinking how citizens data is managed

High-level goals for blue group
- Performance
- Enabling efficiency improvement (like time and cost saving)
- Compatibility
- Usability
- Complying with ethical standard
- Mobile first (Portable)
- Complying with legal and technical regulations and standard (GDPR)
- Blockchain and right to be forgotten and right to rectification
- High level of assurance (trust)
- Security

Figure 7 shows a snapshot of the Miro board after completing Task 1.1.
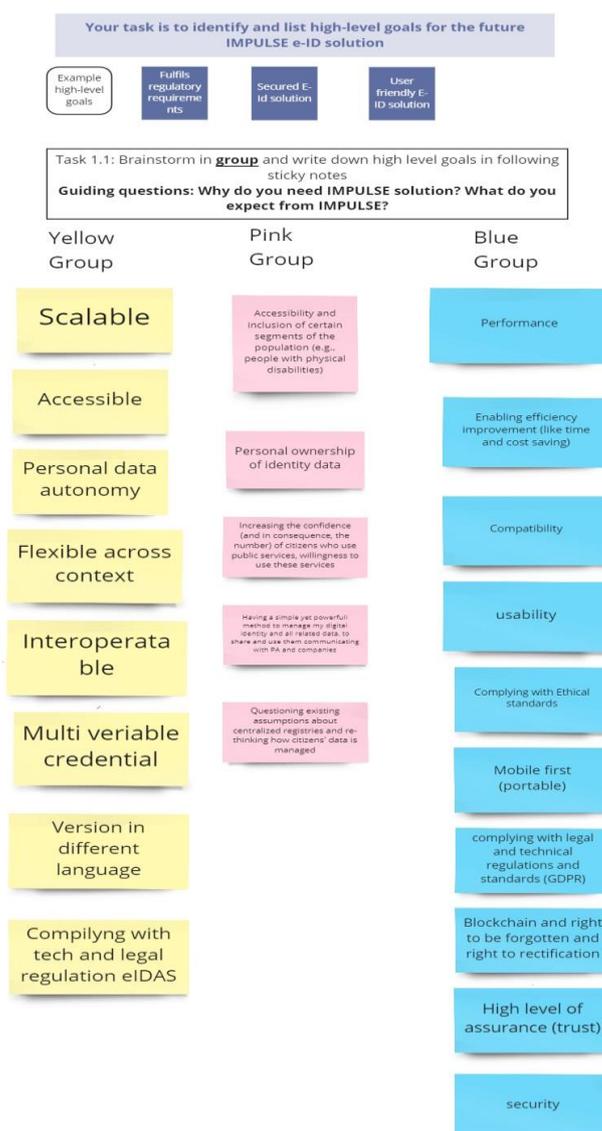
Figure 7: Snapshot of completed task 1.1 for identifying high-level goals

After identifying the high-level goals for the future IMPULSE solution, participants were asked to do the Task 1.2. The participants dragged and dropped similar high-level goals, clustered them, and assigned a meaningful title to the cluster with the help of the facilitators. As a result of this joint discussion, the participants found six category titles:

- Technical robustness
- Compliance to legal regulations, technical and ethical standards
- Accessibility and inclusion by design
- Trust(worthiness)
- Usability and user friendliness
- Security

These six categories were added as headings to the requirements table, so that the participants could refine and validate the requirements found from the literature review.

Task 2: Validating and refining requirements found in the literature through card sorting

The second task for the workshop participants was to validate and refine the requirements found from the literature review. For the first 15 minutes, they had a discussion within their own group and went through 8-9 requirements from the list assigned to their group. In the remaining 10 minutes, all groups rotated through the rest of the requirements from other two groups, so that all participants could have the opportunity to discuss all the requirements originally identified from scientific literature. Then based on the six general level categories named as technical Robustness, compliance to legal regulations, technical and ethical standards, accessibility and inclusion by design, trust(worthiness), usability and user friendliness, security, the participants validated the requirements by putting thumps up to each high-level category. Table 1 shows the yellow group's findings for the requirements validation activity.

Table 1: Yellow group's validated requirements after workshop task 2

Requirements	High-level goal(s)	Reference(s)
The system should keep users' location confidential	Trust(worthiness)	Zirjawi et al., 2015
The system should be interoperable with the legacy (national) e-ID schemes to ensure user uptake.	Technical Robustness, Trust (worthiness)	Bazarhanova et al., 2019
The system should allow reuse of verifiable credentials in the ecosystem.	Accessibility and inclusion by design; Usability, and user friendliness	Bazarhanova et al., 2019
The system should allow users to know how their data would be used and if it is safe from unauthorized access and processing	Security	Wirth et al., 2018
The system should provide short and clear messages and warnings when asking for consent.	Compliance to legal regulations, technical, and ethical standards; Trust(worthiness); Usability and user friendliness	Dhamija & Dusseault, 2008
The system should reveal any personal identifiable information of users only with explicit consent.	Compliance to legal regulations, technical, and ethical standards; Usability and user friendliness; Security	Bazarhanova et al., 2019; Dhamija & Dusseault, 2008
The system should allow users to create, manage, and use his or her identity independently of his or her location and device in use	Technical robustness; Accessibility and inclusion by design; Usability and user friendliness	Alper et al., 2011
The system should maintain users' privacy by improving protection of the users' personal data.	Security	Dhamija & Dusseault, 2008; Zirjawi et al., 2015
The system should indicate to the users where their personal data is stored.	Compliance to legal regulations, technical, and ethical standards; Trust(worthiness)	Stuedi et al., 2010

Figure 8 below shows a snapshot of the collaboration canvas after the yellow group completed the requirements validation activity

Figure 8: Yellow group's validated requirements after workshop task 2

Table 2 below shows the pink group's findings for the requirements validation activity.

Table 2: Pink group's validated requirements after workshop task 2

Requirements	High-level goal(s)	Reference(s)
The system should allow users to control the use of their data in a self-sovereign manner	Compliance to legal regulations, technical and ethical standards, Usability and user friendliness and Security	Dunphy and Petitcolas 2018
The system should allow users to control the information released from the identity provider (IdP).	Usability and user friendliness, Trust (Worthiness)	Alpar et al., 2011
The system should provide seamless identity management for users through a good interface design.	Accessibility and inclusion by design, Usability, and user friendliness	Dhamija & Dusseault, 2008
The system should be easy to download, install, and configure.	Technical robustness, Usability, and user friendliness	Dhamija & Dusseault, 2008

Requirements	High-level goal(s)	Reference(s)
The system should enable time saving features such as automated form filling and single sign-on across the online public services that the user wants to access.	Technical robustness, Usability, and user friendliness	Dhamija & Dusseault, 2008
The system should provide the option to choose a particular identity if the user has multiple identities stored on his or her device when logging to a public service.	*(Participants ran out of time. Validation deferred until next iteration/stage of this deliverable)*	Alpar et al., 2011; Oruaas & Willemson, 2020
The system should simplify the process of updating the user's verifiable credentials (e.g., address changes)	*(Participants ran out of time. Validation deferred until next iteration/stage of this deliverable)*	Alpar et al., 2011
The system should provide simple and well guided user actions when collecting image samples for face recognition	*(Participants ran out of time. Validation deferred until next iteration/stage of this deliverable)*	Tan et al., 2010; Wong et al., 2011

Figure 9 below shows a snapshot of the pink group's collaboration canvas after the requirement validation activity.
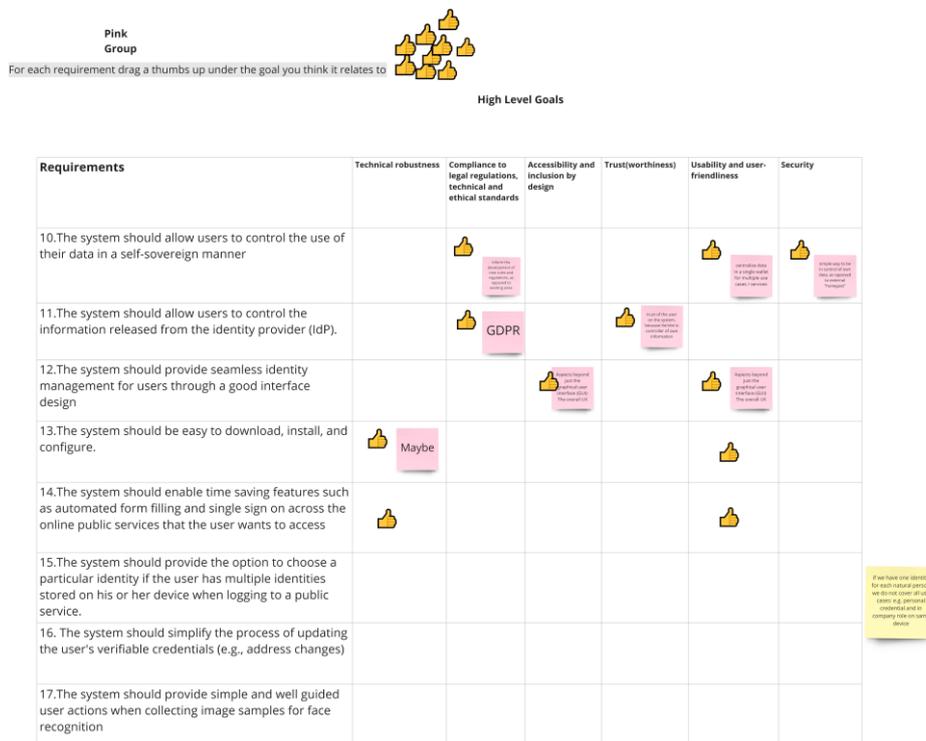
Figure 9: Pink group's validated requirements after workshop task 2

Table 3 shows the blue group's findings for requirements validation.

Table 3: Blue group's validated requirements after workshop task 2

Requirements	High-level goal(s)	Reference(s)
The system should identify the reasons for failure of the authentication process and communicate them to the user.	Usability and user friendliness, Security	Wang et al., 2014
The system should be able to recognize faces captured from images with different resolutions and illumination.	Usability and user friendliness, Trust (Worthiness)	Kamgar et al., 2011
The system should reduce cognitive burden (remembering many user accounts and passwords) for users.	Usability and user friendliness	Dhamija & Dusseault, 2008
The system should allow smart contracts between the citizen and the service provider to establish on how to process the data.	Compliance to legal regulations, technical and ethical standards, Trust (Worthiness)	Bazarhanova et al., 2019
The system should allow removing users' off-chain data if they want.	Compliance to legal regulations, technical and ethical standards	Wirth et al., 2018
The system should use an off-chain solution if blockchain is used for data storage.	Technical robustness, Trust (Worthiness)	Hepp et al., 2018
The system should protect identity information (e.g., fingerprint, facial), which are most critical.	Compliance to legal regulations, technical and ethical standards, trust (Worthiness), Security	Bojinov et al., 2014
The system should protect identity without the need of additional software packages. Users do not want to purchase or use additional software packages to protect identities.	Technical robustness, Compliance to legal regulations, technical and ethical standards	Dhamija & Dusseault, 2008
The system should consider anonymity and pseudo anonymity to be implemented whenever possible	Compliance to legal regulations, technical and ethical standards, Security	Alper et al., 2011; Bazarhavona & Smolander, 2020

Figure 10 below shows a snapshot of the blue group's collaborative whiteboard space after completing the requirements validation activity.

Requirements	Technical robustness	Compliance to legal regulations, technical and ethical standards	Accessibility and inclusion by design	Trust(worthiness)	Usability and user-friendliness	Security
18.The system should identify the reasons for failure of the authentication process and communicate them to the user.					👍	👍
19.The system should be able to recognize faces capture from images with different resolutions and illumination.	👍			👍		
20.The system should reduce cognitive burden (remembering many user accounts and passwords) for users					👍	
21.The system should allow smart contracts between the citizen and the service provider to establish on how to process the data.		👍		👍		
22.The system should allow removing users' off-chain data if they want		👍				
23.The system should use an off-chain solution if blockchain is used for data storage.	👍			👍		
24.The system should protect identity information (e.g., fingerprint, facial), which are most critical		👍		👍		👍
25.The system should protect identity without the need of additional software packages. Users do not want to purchase or use additional software packages to protect identities.	👍	👍				
26.The system should consider anonymity and pseudo anonymity to be implemented whenever possible		👍				👍

Figure 10: Blue group's validated requirements after workshop task 2

Task 3: Identifying additional requirements through user stories

During this task, the yellow group formulated 11 user stories, the pink group formulated 7 user stories and the blue group formulated 10 user stories. These user stories can help the WP5 technical team understand better the user requirements and expectations for the future IMPULSE solution. The user stories created by the workshop participants are listed below.

Yellow group

1. As a citizen, I want a solution that will be going for years, so that I do not need to change my practice
2. As a public administrator, I want a long-lasting solution, so that I can avoid costly projects to change solutions
3. As a legal entity, I want to use the system for my company and for myself with two different credentials, so that I can use it for my company and for my own public services as a citizen without needing multiple devices
4. As a traveller, I want to use a single solution for identifying myself, so that I can have access to all my documents in a single deposit
5. As a citizen, I want to know there is a recovery plan in place if there is a breach of my credentials, so that I can be confident to use Impulse
6. As a citizen, I want to onboard my identity without physically visiting a premise, so that I can do it as and when I need and not only during opening hours
7. As a hacker, I want to crack IMPULSE, so that I have access to all these identities for ever and ever so that I can do nefarious things
8. As a citizen, I want to know who has access to my data, so that I have control over who uses it and for what purpose

9. As a citizen, I want to be actively notified of any changes of the data, so that I know how my data will be used or stored

10. As a victim of an accident, I want to be able to continue to use my account, so that even if I am disfigured in a way that affects recognition

11. As a transgender person, I want a continuity of experience, so that if my facial profile changes that does not affect for authentication

Pink group

1. As citizen/entrepreneur, I want to access public services related to my company, so that I can demonstrate I own that company

2. As a citizen, I want to access a public service by registering only once, so that I can save time and be less error-prone

3. As a public administration, I want citizens to access my services using IMPULSE, so that I can get their identity information

4. As a citizen, I want to access a set of multiple public services and retrieve different information, so that I can reduce the number of steps and save time

5. As a citizen with physical impairments, I want to participate in democratic discussions, so that my opinions and ideas are used for guiding public policymaking

6. As a citizen of MOP, I want to identify myself using IMPULSE, so that I can save costs of acquiring a digital signature

7. As a citizen, I want to receive notifications from the public administrations directly in the IMPULSE app, so that I can be sure that the sender is who he claims to be

Blue group

1. As a European citizen, I want to have a harmonization with the other national ID Providers

2. As a citizen/entrepreneur, I want to share/send only data which are relevant for my purpose, so that I do not have to share all the company data if it is not needed

3. As a citizen, I want to use my IMPULSE digital identity to access all the available digital services in the same way, so that I do not have to manage different ways to access public services (1 app and 1 experience)

4. As a citizen, I want to deactivate my IMPULSE identity in case I lose my mobile (device), so that nobody else can access services instead of me with my digital identity

5. As a European tourist, I want IMPULSE to help, so that I can avoid row (queuing) at airports

6. As a user, I would like that informed consent not only to be a document in legal language, but to be made interactive, so that it is accessible also with dedicated icons

7. As a policy maker, I would like the improvement of public services through IDM, so that it leads to greater political participation. It is not enough to have better comforts to have better democracies

8. If I were a civil and social rights activist, I would like a balance between the right to privacy and social justice issues, so that the access to public services gives us the picture of the new poverty in society

9. As an elderly user I am not very familiar with e-tools, I need a solution that is intuitive to use, so that I do not need extra training on how to use it

10. As a businessperson, I need a solution that is straightforward and not time-consuming to use, so that it does not take a lot of time and efforts to use it

2.4.6   Additional requirements found through user stories

Based on the user stories, we identified 28 additional or new requirements for IMPULSE. Those requirements are listed below and grouped according to their similarity. Whenever possible, the requirements have been clustered under the same six categories defined during the workshop: (1) Technical robustness; (2) compliance to legal regulations, technical, and ethical standards; (3) accessibility and inclusion by design; (4) trust(worthiness); (5) usability and user friendliness; and (6) security.

Based on the analysis of the user stories after the workshops, we have identified 3 requirements that are specific to individual cases; and 4 requirements that are non-verifiable, non-testable, or fall outside the scope of the IMPULSE pilots.

Technical robustness
1. The system should provide citizens with a solution that will be going for years, and the citizens do not need to change the practice
2. The system should provide public administration a long-lasting solution so that public administration can avoid costly projects to upgrade new innovative solutions.
3. The system should let citizens/entrepreneurs share/send data which are relevant for a specific purpose.

Usability and user friendliness
4. The system should provide public administration a better authentication process so that citizens identity information is easy to access for the administration.
5. The system should provide dual identity for a citizen who wants to login for his own company and as a citizen so that login does not require multiple devices and credentials.
6. The system should provide access to all the available digital services so that citizens do not have to manage diverse ways to access public services (1 app and 1 experience).
7. The system should provide an authentication process through which a citizen can access a set of multiple public services and retrieve different information.
8. The system should provide the access to a public service by registering only once so that it takes less time and is less prone to errors.

Accessibility and inclusion by design
9. The system should let citizens to onboard identity without physically visiting a premise, so that the authentication can be done when needed and not only opening hours for the services
10. The system should help to identify citizens using digital signature so that it can save costs of acquiring a digital signature.
11. The system should support special issues of citizens such as a victim of an accident should be able to continue to use the account even if the person is disfigured in a way that affects recognition process.
12. The system should provide a transgender person with an identification experience so that if my facial profile changes that does not affect for authentication.
13. The system should provide elderly citizens a solution that is intuitive to use so that elderly citizens do not need extra training on how to use it.

Compliance to legal regulations, technical, and ethical standards
14. The system should have informed consent not only to be a document in legal language, but to be made interactive so that it is accessible also with dedicated icons
15. The system should notify the citizens any changes of the data so that citizens know how the data will be used or stored.
16. The system should allow citizens to access the data so that they have control over who uses it and for what purpose.
17. The system should provide European citizens a better way to align with the other national ID providers.

Security
18. The system should help a citizen to deactivate personal Identity in case of mobile loss so that nobody can access services with that digital identity.
19. The system should be able to ensure a breach of citizens credentials with a backup plan to adjust the situation.
20. The system should have a good protection so that hackers cannot crack the system and do nefarious things.
21. The system should provide notifications from the public administrations directly in the app so that the identity is trusted and valid.

Case-specific requirements

22. The system should provide citizen/entrepreneur the access to public services to prove their own identity and business profile identity (UC/IC).
23. The system should provide a solution for businessman's that is straightforward and not time-consuming to use so it does not take a lot of time and efforts to use it (UC/IC).
24. The system should provide physically impaired citizens a platform, so that they can participate in democratic discussions and their ideas are used for guiding public policymaking (RVK).

Non-verifiable or outside the scope of IMPULSE pilots

25. The system should guide tourist to avoid row at airports so that the time is saved.
26. The system should provide a traveller single solution for identifying themselves so that travellers can have access to all documents in a single deposit.
27. The system should provide improved public services access to policy makers which could leads to greater political participation. It is not enough to have better comforts to have better democracies.
28. The system should provide civil and social rights activist an authentication process, which will create a balance between the right to privacy and social justice issues, so that the access to public services gives the picture of the new poverty in society

3   Complete list of general requirements for IMPULSE

This section presents the non-exhaustive list of general requirements for the IMPULSE e-ID solution, which were identified during the first stage of the co-creative requirements elicitation process.

Table 4 shows the general requirements identified from the literature review and the validation of those requirements during the co-creation workshop. The validation was done by the project stakeholders that participated in the workshop, who assigned one or more high-level categories to each general requirement. Three general requirements from the literature were not validated due to lack of time during the workshop and will be revised in the next iteration of this deliverable.

Table 5 shows the additional or new requirements from the user stories that were formulated by the project stakeholders during the co-creation workshops. These requirements have been grouped according to their high-level goals and need to be validated in the next stage of the elicitation process. The last column of the table also denotes those requirements from user stories that are related or similar to the ones identified in the initial literature review.

Table 4: Validated requirements from literature review and high-level goals from workshop

No.	General requirements from literature review	High-level goals identified by IMPULSE stakeholders during the validation activity in the workshop
1	The system should keep users' location confidential.	- Trust(worthiness)
2	The system should be interoperable with the legacy (national) e-ID schemes to ensure user uptake.	- Technical Robustness - Trust(worthiness)
3	The system should allow reuse of verifiable credentials in the ecosystem.	- Accessibility and inclusion by design - Usability, and user friendliness
4	The system should allow users to know how their data would be used and if it is safe from unauthorized access and processing.	- Security
5	The system should provide short and clear messages and warnings when asking for consent.	- Compliance to legal regulations, technical and ethical standards - Trust(worthiness) - Usability and user friendliness
6	The system should keep users' location confidential	- Trust(worthiness)
7	The system should allow users to control the use of their data in a self-sovereign manner.	- Compliance to legal regulations, technical and ethical standards - Usability and user friendliness - Security
8	The system should allow users to control the information released from the identity provider (IdP).	- Usability and user friendliness, - Trust(worthiness)
9	The system should provide seamless identity management for users through a good interface design.	- Accessibility and inclusion by design - Usability, and user friendliness
10	The system should be easy to download, install, and configure.	- Technical robustness - Usability, and user friendliness
11	The system should enable time saving features such as automated form filling and single sign-on across the online public services that the user wants to access.	- Technical robustness - Usability, and user friendliness

12	The system should provide the option to choose a particular identity if the user has multiple identities stored on his or her device when logging to a public service.	- *(Participants ran out of time. Validation deferred until next iteration/stage of this deliverable)*
13	The system should simplify the process of updating the user's verifiable credentials (e.g., address changes).	- *(Participants ran out of time. Validation deferred until next iteration/stage of this deliverable)*
14	The system should provide simple and well guided user actions when collecting image samples for face recognition.	- *(Participants ran out of time. Validation deferred until next iteration/stage of this deliverable)*
15	The system should identify the reasons for failure of the authentication process and communicate them to the user.	- Usability and user friendliness, Security
16	The system should be able to recognize faces captured from images with different resolutions and illumination.	- Usability and user friendliness, - Trust(worthiness)
17	The system should reduce cognitive burden (remembering many user accounts and passwords) for users.	- Usability and user friendliness
18	The system should allow smart contracts between the citizen and the service provider to establish on how to process the data.	- Compliance to legal regulations, technical and ethical standards - Trust(worthiness)
19	The system should allow removing users' off-chain data if they want.	- Compliance to legal regulations, technical and ethical standards
20	The system should use an off-chain solution if blockchain is used for data storage.	- Technical robustness - Trust(worthiness)
21	The system should protect identity information (e.g., fingerprint, facial), which are most critical.	- Compliance to legal regulations, technical and ethical standards - Trust(worthiness) - Security
22	The system should protect identity without the need of additional software packages. Users do not want to purchase or use additional software packages to protect identities.	- Technical robustness - Compliance to legal regulations, technical and ethical standards
23	The system should consider anonymity and pseudo anonymity to be implemented whenever possible.	- Compliance to legal regulations, technical and ethical standards, Security

Table 5: Additional or new requirements formulated through user stories (to be validated later)

High-level goals identified by IMPULSE stakeholders	Additional or new requirements proposed through user stores	Similar or related general requirements from literature (Table 4)
Technical robustness	The system should provide citizens with a solution that will be going for years, and the citizens do not need to change the practice	2
	The system should provide public administration a long-lasting solution so that public administration can avoid costly projects to upgrade new innovative solutions.	2

High-level goals identified by IMPULSE stakeholders	Additional or new requirements proposed through user stores	Similar or related general requirements from literature (Table 4)
	The system should let citizens/entrepreneurs share/send data which are relevant for a specific purpose.	4
Usability and user friendliness	The system should provide public administration a better authentication process so that citizens identity information is easy to access for the administration.	
	The system should provide dual identity for a citizen who wants to login for his own company and as a citizen so that login does not require multiple devices and credentials.	3
	The system should provide access to all the available digital services so that citizens do not have to manage diverse ways to access public services (1 app and 1 experience).	3
	The system should provide an authentication process through which a citizen can access a set of multiple public services and retrieve different information.	3
	The system should provide the access to a public service by registering only once so that it takes less time and is less prone to errors.	3
Accessibility and inclusion by design	The system should let citizens to onboard identity without physically visiting a premise so that the authentication can be done when needed and not only opening hours for the services	
	The system should help to identify citizens using digital signature so that it can save costs of acquiring a digital signature.	
	The system should support special issues of citizens such as a victim of an accident should be able to continue to use the account even if the person is disfigured in a way that affects recognition process.	
	The system should provide a transgender person with an identification experience so that if my facial profile changes that does not affect for authentication.	
	The system should provide elderly citizens a solution that is intuitive to use so that elderly citizens do not need extra training on how to use it.	

High-level goals identified by IMPULSE stakeholders	Additional or new requirements proposed through user stores	Similar or related general requirements from literature (Table 4)
Compliance to legal regulations, technical, and ethical standards	The system should have informed consent not only to be a document in legal language, but to be made interactive so that it is accessible also with dedicated icons	5
	The system should notify the citizens any changes of the data so that citizens know how the data will be used or stored.	4, 18
	The system should allow citizens to access the data so that they have control over who uses it and for what purpose.	4, 18
	The system should provide European citizens a better way to align with the other national ID providers.	2, 3
Security	The system should help a citizen to deactivate personal identity in case of mobile loss so that nobody can access services with that digital identity.	
	The system should be able to ensure a breach of citizens credentials with a backup plan to adjust the situation.	
	The system should have a good protection so that hackers cannot crack the system and do nefarious things.	
	The system should provide notifications from the public administrations directly in the app so that the identity is trusted and valid.	

4   Limitations and future activities

4.1 Limitations of the initial stage of requirements elicitation

The workshop was conducted online, relying on Microsoft Teams and Miro as main tools to mediate the communication, instruction, and interaction with the participants. If the workshop had taken place in a physical setting under a normal context without the COVID-19 pandemic restrictions, the number of participants might have been higher, and the interactions among those participants would have been more engaging and livelier. Therefore, some of the limitations of the first stage of the co-creative requirements elicitation process were the asynchronous nature of most communications and the exchange of thoughts, views, and ideas of the participants through a virtual environment only.

Another important limitation of the initial stage of requirements elicitation was the absence of citizens, who were not directly involved in the IMPULSE Consortium. Due to pandemic situation, the uncertainties in the definition of the six pilot cases, and the lack of agreed procedures for personal data collection and sharing, it was deemed non-essential and risky to invite "regular outside" citizens at this early phase in the process. For subsequent stages and iterations of this deliverable, the active involvement of more citizens without prior knowledge of IMPULSE.

Finally, in the online co-creation workshop conducted for the elicitation of general requirements, we identified a non-exhaustive list of requirements, in addition to those from the scientific literature, which should be further validated, augmented, or refined in the next stages of the co-creative process.

4.2 Future steps

The future workshops will be conducted with case owners, stakeholders, representatives of public administrations, and citizens from the six pilot cases. One of the core principles of IMPULSE is the active involvement of citizens in the pre-piloting and piloting activities. The case representatives will support in the recruitment of participants for the future workshops through additional and more public communication channels. We expect that the next co-creation workshops can be conducted in a physical setting after the pandemic has receded.

5 Conclusions

The deliverable summarizes the activities of co-creative requirements elicitation that were conducted during the first seven months of IMPULSE. These activities comprised a literature review on general requirements and co-creation methods, as well as an online workshop.

The co-creation workshop involved representatives from all six pilot cases, who validated and refined the requirements from scientific literature. The workshop activities also allowed to identify additional requirements, which can help the WP5 technical team understand better what the user needs for the future IMPULSE e-ID solution will be so that users who could use IMPULSE will get the benefit. Finally, the list of general requirements presented in this deliverable D2.2 shall be augmented, refined, and prioritized in the subsequent stages of the elicitation process.

References

- Alpár, G., Hoepman, J. H., & Siljee, J. (2011). The identity crisis. security, privacy and usability issues in identity management. arXiv preprint arXiv:1101.0427.

- Alper, B., Riche, N., Ramos, G., & Czerwinski, M. (2011). Design study of linesets, a novel set visualization technique. *IEEE transactions on visualization and computer graphics*, *17*(12), 2259-2267.

- Bazarhanova, A., & Smolander, K. (2020). The review of non-technical assumptions in digital identity architectures. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Hawaii, USA.

- Bazarhanova, A., Magnusson, J., Lindman, J., Chou, E., & Nilsson, A. (2019). Blockchain-based electronic identification: cross-country comparison of six design choices. In Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden.

- Bojinov, H., Michalevsky, Y., Nakibly, G., & Boneh, D. (2014). Mobile device identification via sensor fingerprinting. arXiv preprint arXiv:1408.1416.

- Clancy, T. C., Kiyavash, N., & Lin, D. J. (2003). Secure smartcard-based fingerprint authentication. In Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications.

- Dhamija, R., & Dusseault, L. (2008). The seven flaws of identity management: Usability and security challenges. *IEEE Security & Privacy*, 6(2), 24-29.

- Hadid, A., Heikkila, J. Y., Silvén, O., & Pietikainen, M. (2007). Face and eye detection for person authentication in mobile phones. In 2007 ACM/IEEE International Conference on Distributed Smart Cameras, Vienna, Austria.

- Hannah, S. (2008). Sorting out card sorting: Comparing methods for information architects, usability specialists, and other practitioners. Accessed from https://core.ac.uk/download/pdf/36682881.pdf on 30th August 2021.

- Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR compliant Blockchains–A systematic literature review. *IEEE Access*, 9, 50593-50606.

- Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K. (2018). E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, Canada.

- Hedström, K., Wihlborg, E., Gustafsson, M. and Söderström, F. (2015). Constructing identities – professional use of e-ID in public organisations. *Transforming Government: People, Process and Policy*, 9(2), 143-158.

- Hepp, T., Sharinghousen, M., Ehret, P., Schoenhals, A., & Gipp, B. (2018). On-chain vs. off-chain storage for supply-and blockchain integration. *it-Information Technology*, 60(5-6), 283-291.

- Kamgar-Parsi, B., Lawson, W., & Kamgar-Parsi, B. (2011). Toward development of a face recognition system for watchlist surveillance. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(10), 1925-1937.

- Lirginlal, D. and Phelps, D. (2012). Tracking the socio-technical barriers to digital identity adoption in Arab countries: A case study of Qatar. In 9th International Conference on E-Governance, Cochin, India.

- Liu, J., Cao, H., Li, Q., Cai, F., Du, X., & Guizani, M. (2018). A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing. *IEEE Internet of things Journal*, 6(2), 1321-1330.

- Lucassen, G., Dalpiaz, F., Van Der Werf, J. M. E., & Brinkkemper, S. (2015). Forging high-quality user stories: towards a discipline for agile requirements. In 2015 IEEE 23rd international requirements engineering conference (RE), Ottawa, Canada.

- Oruaas M., Willemson J. (2020). Developing Requirements for the New Encryption Mechanisms in the Estonian e-ID Infrastructure. In: Robal T., Haav HM., Penjam J., Matulevičius R. (eds)

Databases and Information Systems. DB&IS 2020. Communications in Computer and Information Science, vol 1243. Springer, Cham.

- Spencer, D., & Warfel, T. (2004). Card sorting: a definitive guide. *Boxes and arrows*, *2*, 1-23.

- Stuedi, P., Mohomed, I., & Terry, D. (2010). Wherestore: Location-based data storage for mobile devices interacting with the cloud. In Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond.

- Tan, X., & Triggs, B. (2010). Enhanced local texture feature sets for face recognition under difficult lighting conditions. *IEEE Transactions on Image Processing*, 19(6), 1635-1650.

- Tsap, V., Pappel, I., & Draheim, D. (2019). Factors affecting e-ID public acceptance: a literature review. In International Conference on Electronic Government and the Information Systems Perspective (pp. 176-188). Springer, Cham.

- Turner, A. M., Reeder, B., & Ramey, J. (2013). Scenarios, personas and user stories: User-centered evidence-based design representations of communicable disease investigations. *Journal of Biomedical Informatics*, 46(4), 575-584.

- Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2011). Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on Computers*, 62(2), 362-375.

- Wang, D., & Wang, P. (2014). Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. *Ad Hoc Networks*, 20, 1-15.

- Wayman J., Jain A., Maltoni D., Maio D. (2005) An Introduction to Biometric Authentication Systems. In: Wayman J., Jain A., Maltoni D., Maio D. (eds) Biometric Systems. Springer, London.

- Wirth, C., & Kolain, M. (2018). Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data. In Proceedings of 1st ERCIM Blockchain Workshop. European Society for Socially Embedded Technologies (EUSSET).

- Wong, Y., Chen, S., Mau, S., Sanderson, C., & Lovell, B. C. (2011). Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition. In CVPR 2011 WORKSHOPS, Colorado Springs, CO, USA.

Zirjawi, N., Kurtanovic, Z., & Maalej, W. (2015). A survey about user requirements for biometric authentication on smartphones. In IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE), Ottawa, Canada.