Impulse

Identity Management in PUbLic SErvices

D6.4 Analytical Report

Lead Author: Bertille Auvray (TES)

With contributions from: Jiri Musto (LUT), Bernd Beckert (Fh ISI)

Reviewer: Bernd Beckert (Fh ISI), Jakob Asmussen (ARH)

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Delivery date:	15-02-2024
Version:	3
Total number of pages:	45
Keywords:	Roadmap, Recommendations, Open Community, Transferability

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

Executive summary

IMPULSE intends to be a novel electronic identity management (eID) system to be integrated into the online public services as a new and alternative eID option. Unlike other centralized eID systems like the ones based on user/password or federated identities (i.e., Facebook, Google, LinkedIn…), IMPULSE proposes a secure and privacy preserving alternative for the existing eID management systems, being the self-sovereign identity (SSI) concept at the core of the user-centric IMPULSE eID approach. By combining existing and disruptive technologies such as Artificial Intelligence (AI), Blockchain and Smart Contracts, IMPULSE intends to transform the two critical processes to get access to online public services: the enrolment and authentication processes.

In addition to developing, programming and testing the IMPULSE solution in the technical and piloting parts of the project, we have analysed the possibilities and barriers for the IMPULSE solution to be utilised in the future. In WP6: "Roadmapping for adoption, escalation and sustainability" we have analysed the options for adopting, upscaling and sustainably implementing the IMPULSE-system under the conditions in the countries involved in the project.

This report details the strategic roadmaps and shows requirements and possible action points needed by future adopters of the IMPULSE solution. The report draws from all tasks of WP6, including the discussions with the associated Digital Innovation Hubs (D6.1), the six dissemination workshops (D6.2) and the roadmapping exercise for the further development and deployment of the IMPULSE solution (D6.2). The report also takes up important insights from the technical deliverables, especially when addressing issues to overcome the identified barriers. While the roadmaps depicted in D6.2 shall serve as an overview of what should happen next, this analytical report draws together all the findings and gives a detailed description of the activities to be considered when trying to establish IMPULSE in different settings.

One important insight is that the question of the adoption and continuation of the IMPULSE-solution and its necessary requirements cannot be answered in the same way for all countries. In the IMPULSE-project, stakeholders from eight countries were involved and pilots were developed and implemented in five countries (Denmark, Iceland, Spain, Italy, Bulgaria). In the participating countries, there are different starting conditions for the possibilities to adopt and continue the IMPULSE solution. Thus we have clustered the different countries into three groups: Leaders, followers and latecomers. For each group, we detail the needs and requirements for the further adoption of the IMPULSE-solution.

This information is complemented by specifying future activities from a technical point of view. In chapter 3 of this report we show in a detailed manner the technical requirements and the barriers which need to be overcome in the future to take the project results from the pilots to the next level.

In the conclusion we provide country-specific next steps for the future implementation of IMPULSE, including very concrete activities that we hope will be taken up in a follow-up process or project to make further use of the IMPULSE results.

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**	D6.4	**Title**	Analytical report
Work package	**Number**	WP6	**Title**	Roadmapping for adoption, escalation and sustainability
Task	**Number**	T6.4	**Title**	Analytical report explaining the roadmaps

Date of delivery	**Contractual**	M36	**Actual**	M37
Status	version 3		☐Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)	Bertille Auvray (TES)			
Responsible author	**Name**	Bertille Auvray		
	Partner	TES	**E-mail**	bertille.auvray@pole-tes.com

Summary (for dissemination)	One of WP6 goals is create roadmaps for the adoption, adaptation and development of the IMPULSE solution, relying on the partners' contact networks, the DIHs participating in the Digital Innovation Board (DIB) and the experts on the Advisory Board (AB). Within this work package, the development of 6 specific roadmaps and one EU roadmap is intended to help partners gather more information, to enable a simple and clear visualisation of the solution being tested in the project and to promote the adoption and/or adaptation of the IMPULSE initiative in European countries. Alongside those roadmaps, an analytical report is written. The latter provides more details on the strategic roadmaps, action points and requirements for future users of IMPULSE or similar solutions. Based partly on further desk-based research and partly on research outputs from previous WPs and T6.2 and T6.3, it details goals, gaps and barriers and how to overcome them, milestones, action items and timelines. Finally, the cross-feeding of the 6 pilot experiments, together with the contribution of the community set up as part of the T6.1 project, is intended to optimise the applicability and transferability of the project's results to a long-term road mapping product.
Keywords	Roadmap, Recommendations, Open Community, Transferability

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
25/01/2024	1	Bertille Auvray (TES)	Complete document draft for revision
30/01/2024	2	Bernd Beckert (Fh ISI)	Official Review
01/02/2024	2	Alicia Jiménez (GRAD)	Deliverable review for comments
02/02/2024	2	Jakob Asmussen (ARH)	Official review
09/02/2024	3	Bertille Auvray (TES)	Final deliverable version for submission

Table of contents

List of figures

List of tables

Abbreviations and acronyms

AB: Advisory Board
AEI : Agency for European Integration and Economic Development
AI: Artificial intelligence
ARH: City of Aarhus, Denmark
BDIH: Basque Digital Innovation Hub
CEI: Call for expression of interest
CEL: CyberEthics Lab. Srls
dApps: Decentralized Applications
DEP: Digital Europe Programme
DIB: Digital Innovation Board
DIH: Digital Innovation Hub
DIN: Deutsches Institut für Normung e. V.
DoA: Description of action (IMPULSE project)
Dx.x: Deliverable
EDIH: European Digital Innovation Hub
e-ID: Electronic identification
ERTZ: Basque Government – Security Department – Ertzaintza
Fh ISI: Fraunhofer Institute for Systems and Innovation Research
GIJON: City of Gijón, Spain
GRAD: Fundación Centro Tecnolóxico de Telecomunicacións de Galicia
ICERT: Infocert S.p.A.
ICT: Information and Communication Technologies
LUT: Lappeenrannan-Lahden Teknillinen Yliopisto
MOP: Municipality of Peshtera, Bulgaria
NGO: Non-Governmental Organization
PAs: Public administration-s
RTOs: Research and Technology Organisations
RVK: City of Reykjavik, Iceland
STP: Sofia Tech Park
TES: Association du Pole de Competitivite Transactions Electroniques Securisees – DIH
TREE: Tree Technology SA
Tx.x: Task
UC/IC: Union of Italian Chambers of Commerce / InfoCamere
UNE: Asociación Española de Normalización
WP: Work package (IMPULSE DoA)
WG: Working Group

1 Introduction

1.1 Reminder of the task

IMPULSE is carrying out a user-centric and multidisciplinary impact analysis on the integration of blockchain and AI for eID in public services. The project is evaluating the benefits but also the risks, costs, and limitations of the integration of such technologies in this context. At European level, this means that cross-border access, security, and adaptability will have to be guaranteed to ensure the solution's marketability.

Within the structure of the project, WP6 focuses its work on the wider opening of the project to a more general theme: the use of new eID technologies in public services and business contexts. Thus, this WP aims both at creating several local communities in different European countries around this topic and to manage them; but also to build on the experience of the IMPULSE project, and more particularly of the 6 case studies, to try and encourage the implementation of these innovative technologies in the widest possible way, through the IMPULSE solution and related ones.

Specifically, Task 6.4 focuses on explaining and detailing the six country roadmaps and the European roadmap developed within Task 6.3.

1.2 Aim of the deliverable

The aim of this deliverable is to detail the strategic roadmaps on the key points, to pool the action points and requirements necessary for the future users of a solution such as IMPULSE and to consult the rest of the project work for this purpose.

Apart from the discussions with the associated Digital Innovation Hubs (D6.1), the report also draws from other tasks of WP6, including the six dissemination workshops (D6.2), and the roadmapping exercise for the further development and deployment of the IMPULSE solution (D6.3). The report also takes up important insights from the technical deliverables, especially when addressing issues to overcome identified barriers. This deliverable aims to present the activities carried out on stakeholders' engagement and community management, beyond the participating partners, as well as the result of the set up strategy in terms of communication and community expansion. This deliverable is the end of the project update.

1.3 Relation to the whole project

D6.4 aligns with the following goals and specific objectives defined in the IMPULSE DoA:

In summary, D6.4 contribution to IMPULSE is:

- The explanation of the roadmaps
- Provide further information to complete the content of the roadmaps, allowing them to remain concise

1.4 Document architecture

This deliverable is divided into 2 main parts:

- Part 1 is dedicated to identifying needs, demands and requirement for further adoption of the IMPULSE solution, such as maturity, technology understanding, ethics and engagement (Chapter 2, 3, 4 and 5)
- Part 2 is focusing on the project's aftermath and what remains to be taken into account (Chapter 6)

2 Needs, demands, and requirements for further adoption of the IMPULSE-solution

2.1 Level of maturity

The level of digital maturity is an important factor to take into account when it comes to implementing a (new) solution, as this constitutes a starting point to consider especially to better understand the different needs the IMPULSE pilots may have.

In the case of the IMPULSE project, we are dealing with eight different countries:

- five pilot countries – Iceland, Denmark, Spain, Bulgaria and Italy
- and three partner countries – France, Germany and Finland.

As it has been stated in D6.2, the current state of the use of eIDs in these countries is quite different:

Table 1: Use of eIDs in selected countries in 2023

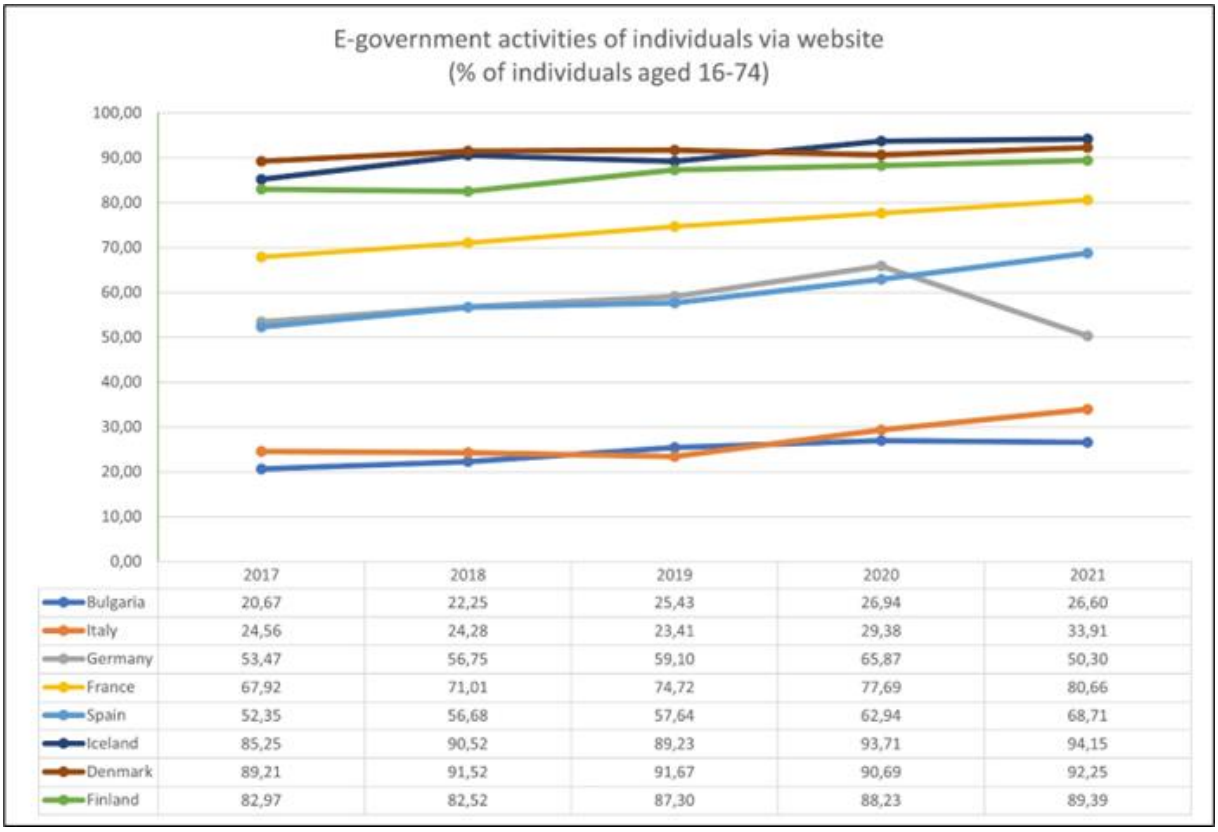
Country	Use of eIDs in the population (estimates)
Denmark, Iceland, Finland	80-90%
Spain	over 40% in certain regions with local eID schemes, national eID use is below 10%
France	below 10%, but increasing
Italy	
Germany	
Bulgaria	in early stage

Source: *Own compilation based on the country reports, see D6.2*

Further research has been done within this deliverable, in order to refine those groups into three mains one, based on:

- The level of e-government activities of individuals via website
- The type of identification process used to access online public services
- The Digital Economy and Society Index data

2.1.1 E-government activities of individuals via website



	2017	2018	2019	2020	2021
Bulgaria	20,67	22,25	25,43	26,94	26,60
Italy	24,56	24,28	23,41	29,38	33,91
Germany	53,47	56,75	59,10	65,87	50,30
France	67,92	71,01	74,72	77,69	80,66
Spain	52,35	56,68	57,64	62,94	68,71
Iceland	85,25	90,52	89,23	93,71	94,15
Denmark	89,21	91,52	91,67	90,69	92,25
Finland	82,97	82,52	87,30	88,23	89,39

Figure 1 E-government activities of individuals via website - Source: Eurostat isoc_ciegi_ac

There is a difference between the percentage of individuals who carry out e-government activities (electronic government or the dematerialisation of public services) online via a website:

- At the top of the rankings are Denmark, Iceland and Finland, which had the most e-government interactions in 2017. More than 80% of individuals and even more than 90% for Iceland and Denmark in 2021 (with Finland a very close second at 89%).
- In the middle of the pack are France, Germany, and Spain, with a steady increase (+12 points for France between 2017 and 2021, or +16 points for Spain over the same period).
- Italy and Bulgaria are further down the list. However, Italy implemented a functioning solution, the SPID (Public Digital Identity System) with a decree dated from 24 October 2014 and notified in 2018. After that, the number of digital identities issued exceeds 25 million, with an increase of 61.5% in 2021.

2.1.2 Identification procedures used for online services

Dataset: **Identification procedures used for online services (2020 onwards) [isoc_cisci_ip20]**
Last updated: 15/12/2023 11:00

Time frequency Annual
Individual type All individuals aged 16-74
Unit of measure % per individuals
Time 2022

	Individuals used simple login with username and password as identification procedure for accessing online services	Individuals used electronic identification certificate or card with a card reader or an app as identification procedure for accessing online services	Individuals used a procedure involving their mobile phone (a code received via a message) as identification procedure for accessing online services	Individuals used single use pin code list or random characters of a password as identification procedure for accessing online services	Individuals have not used any electronic identification procedure for accessing online services
Bulgaria	53,79	3,09	9,30	1,29	14,08
Denmark	72,17	50,16	76,26	83,78	1,98
Finland	72,10	2,77	58,31	66,99	2,18
France	:	:	:	:	:
Germany	85,26	22,47	46,18	26,81	5,89
Iceland	90,04	92,89	79,99	21,56	:
Italy	65,44	9,31	38,48	16,03	:
Spain	77,98	22,89	60,80	32,13	11,21

Special value
: not available

Figure 2 Identification procedures used for online services - Source: Eurostat isoc_cisci_ip20

When it comes to the means used to access public services online, there are still disparities between countries. There is still massive use of the simple code and password, or of the unique code in 2022 by all countries. However, we can note the use of electronic identification certificates via a card reader or an app as a means of identification (as for IMPULSE) in Iceland and Denmark, or at least dual identification for the others. The exception is Bulgaria, where mainly simple passwords are used, and where no electronic identification service is used at all (14% of respondents aged 16-74).

It can be noted that in IMPULSE, when we talk about eID, we are talking about a personal digital ID enabling people to identify themselves and use online public services, without having to go anywhere to prove their identity, thanks to a secure identification process using facial biometric recognition. IMPULSE would then fall more into the category of "*Individuals used electronic identification certificate or card with a card reader or an app as identification procedure for accessing online services*".

2.1.3 Digital Economy and Society Index

Finally, according to the DESI (Digital Economy and Society Index), summarising indicators on Europe's digital performance and tracked the progress of EU countries, from 2014 to 2022:

Table 2 Combined data from DESI Countries' performance in digitisation

DESI 2022	e-Gov users	Digital public services for citizens	EU rank
Bulgaria	34%	76%	25
Denmark	93%	83%	8
Finland	92%	90%	2
France	87%	69%	15
Germany	55%	76%	18
Iceland	:	:	:
Italy	40%	67%	19
Spain	73%	87%	5
EU	**65%**	**75%**	/27

When it comes to digital public services, **Finland** ranks second among EU countries and scores well above the European average. Online interaction between government authorities and the public is approaching peak levels with 92% of Finnish internet users using e-government services. According to the overall data used to determine the country performance in digitisation, Finland ranks 2nd out of 27 European countries.

Denmark, meanwhile, has been a forerunner in the digitisation of the public sector for many years. Today, essential public service solutions that can be digitised are provided online. The digitisation of public self-service solutions was made compulsory by law in 2012. According to the overall data used to determine the country performance in digitisation, Denmark ranks 8th out of 27 European countries.

Italy ranks 19th in the EU for digital public services. Despite steady progress, only 40% of Italian internet users use digital public services, well below the EU average of 65%. Nevertheless, take-up of the "SPID" electronic identification system has continued to rise (over 29.4 million SPIDs issued by 2022), and over 27 million people had a "CIE" (Carta di Identità Elettronica) national identity card, equipped with a contactless chip enabling the access to online services. According to the overall data used to determine the country performance in digitisation, Italy ranks 19th out of 27 European countries.

Spain is at the forefront of e-government and digital public services in the EU. It continues to update its services and infrastructures to adapt them to the needs of citizens and businesses and to the rapid evolution of technologies. In addition, interoperability at national, regional and local level will be essential to ensure a smooth and efficient digital transition between the different levels of government, optimising resources and avoiding duplication. According to the overall data used to determine the country performance in digitisation, Spain ranks 5th out of 27 European countries.

France is already performing well in the provision of digital public services, for example in terms of e-government users, with 87% of internet users using online public services, compared to an EU average of 65%. However, its performance is slightly below average when it comes to digital public services for citizens, which means that its efforts need to be sustained to ensure that services for citizens are more effective and as widely adopted as possible. According to the overall data used to determine the country performance in digitisation, France ranks 15th out of 27 European countries.

Germany ranks 18th in the EU for digital public services. The country is still falling short of expectations in this area, despite several initiatives by the federal government to speed up the digitisation of public services. Numerous initiatives have been launched over the years to roll out digital public services. If the measures are implemented effectively and on time, they should make it possible to improve the indicators concerned.

According to the overall data used to determine the country performance in digitisation, Germany ranks 18th out of 27 European countries.

As far as **Bulgaria** is concerned, the country performs rather poorly when it comes to digital public services, ranking 25th in the EU. Although the country has many public services already online and has launched several initiatives to digitise even more public services, these have not had any tangible effect on its DESI performance. According to the overall data used to determine the country performance in digitisation, Bulgaria ranks 25th out of 27 European countries.

2.1.4 Digital Maturity Assessment

Based on the previous research, project results and new desk-based research, countries can be grouped in different families to reflect on their level of maturity regarding eID. To better visualise this, they have been placed on a maturity level line based on a digital maturity model.

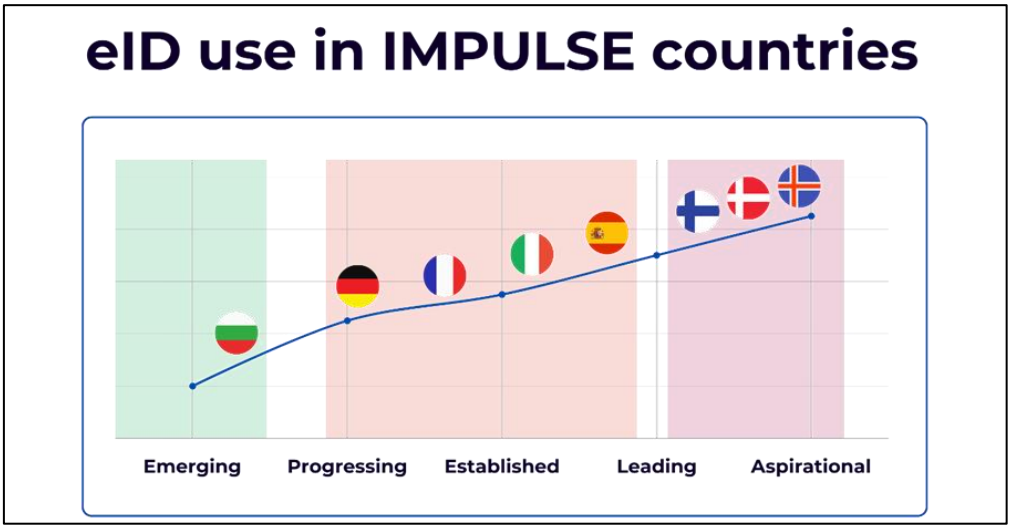


Figure 3 Based on DIGITAL TRANSFORMATION MATURITY MODEL © OECD 2022[1]

2.1.5 Final overview

As a summary and conclusion:

	LEADERS	FOLLOWERS	LATECOMERS
Countries	Denmark, Finland, Iceland	Italy, Spain, Germany, France	Bulgaria
Maturity	Aspirational / Leading	Progressing / Established	Emerging
eID-situation	eID is available and widely used.	eID is available (to a certain extend) with a low but growing use.	No efficient eID available or usage of sectoral eIDs.
E-Government-services situation	Many e-Gov-services available and widely used by citizens	An increasing number of e-Gov-services available but use of services by citizens is relatively low	Although there is an increasing number of E-gov-services offered their use by citizens is low.

[1] OECD (2022), Digital Transformation Maturity Model, OECD, Paris. www.oecd.org/tax/forum-on-tax-administration/publications-and-products/digital-transformation-maturity-model.htm

Note to the readers: It is highly important to note and keep in mind that this does not in any way reflect the capabilities of the country or the pilot case; it is not a ranking from best to worst. This research and report are not intended to be critical, but simply to take stock of the situation.

2.2 Initial needs and requirements from the pilots

In line with the previous point highlighting the differences between countries in terms of maturity of use and access to online public services, this section details the situation in the three country groups (leaders, followers, latecomers). We look at the different needs and requirements in the three groups with respect to the adoption of the IMPULSE solution. The following analysis is based on experiences collected in the pilots, on the contributions by the participants of the workshops and on insights from the roadmapping exercise.

2.2.1 Needs

- **Leaders**

In the group known as leaders, the idea behind IMPULSE pilots was to target people with special needs to ensure that the whole population can be included and that no one is left out of public services: For **Aarhus (Denmark)**, the aim was to explore how the IMPULSE solution can improve current services for vulnerable citizens as a user-friendly solution to allow both the retrieval of the paper code card (e.g., access to safe storage) and a more flexible digital alternative to apply for services. Please note that this describes the starting point for the Aarhus case; however, there have been changes both in the target audience for the case and in relation to the new eID introduced during the project period.

For the **City of Reykjavik (Iceland)**, the aim was to deploy and evaluate IMPULSE as an advanced solution for e-government and other services using facial recognition which can easily be accessed also by disabled persons.

In addition to these social and inclusion-oriented needs, needs of a more general nature emerged over the course of the project. The following aspects are particularly important in the leaders group with regard to a possible introduction of the IMPULSE solution:

- **User onboarding of persons, not being citizens of the Nordics.** Existing eID systems in Denmark, Iceland and Finland use central databases where personal numbers of their citizens are stored for authentication. Foreigners and expats do not have a personal citizen number in these countries, thus there is a need to implement alternative onboarding processes that enable this group of people to use the same services as citizens of the Nordics. The IMPULSE-solution could be a solution to address this need.
- **Moving from password-based to eID systems.** In countries where eID-systems are already in place and widely used there is a general need to make these systems more user-friendly. This could include the replacement of passwords by facial-recognition authentication. For leaders this seems to be the next natural step forward and IMPULSE could provide the respective solution.
- **User onboarding without having to show up in person.** This is another natural next step for the leader countries and could increase user-friendliness and acceptance rates even more. Currently, citizens have to show up in person at authorized offices (at public administration, dedicated service points, banks, telephone shops etc.) for a formal first-time identification. If the onboarding was done via IMPULSE eliminating the need to visit these points, this would address another important need in these countries.

- **Integrate e-health and share health data in the system.** eID systems become more attractive for users the more services are accessible through them. This applies in particular to healthcare services, which are still largely separate even in the leading countries, as they often use their own access systems. Health data is particularly worthy of protection, which is why the requirements for the security and trustworthiness of the access system are particularly high. The IMPULSE solution could be an adequate answer here.
- **How will a common EU eID look like?** Countries where eID-systems are already available and integrated in every-day lives of citizens are aware of the importance of coordination when introducing such a system. They ask themselves how a unique unifier (as the Nordics have) could be set up in Europe. Another need in this context is to ensure compatibility of a future European standard eID with the national eID-systems that are already in place.

➢ **Followers**

For the followers, the question is how to specifically improve existing solutions or how to supplement them to make them more functional. For example, for the **City of Gijon (Spain)**, the aim of the pilot was to explore an identification alternative of their physical citizen card (using code and pin number) to access the digital services they provide. For **Ertzaintza (Spain)**, the pilot aimed at enabling secure and trustworthy eID so that complaint processes could be entirely completed online using IMPULSE once the citizen filled in the form on the ERTZ web page, and just before the information is submitted to the Police Management Service.

Lastly, for **UnionCamere (Italy)**, it was important to assess how IMPULSE could transform the authentication process, making it secure and transparent by design, preserving data hosting on trusted sources while providing full flow control to the business persons on their own data.

In addition to the specific needs emerging from gaps or missing features in existing eID-systems, more general needs with regard to the possible adoption of the IMPULSE solution were identified in the group of the followers:

E-gov services wanted especially in rural areas. A special need for eID-systems exists in rural areas where administrative and business infrastructure is weak. Citizens living in rural areas should be able to participate in public and business activities as well as people living in urban areas. They should be able to access all services over the Internet. eIDs can help to meet this need, especially those systems that are user-friendly, secure and reliable. One access point for support in using eIDs, especially for the elderly, could be the notary's offices which still exist in rural areas.

- **Integrating different services into the eID-system.** The more services to access via the eID-system, the more attractive it is for the users. Apart from e-government services they could include payment functions, access to health services or welfare benefits and many other services. Adding different services which can be used by the eID system is a clear demand in countries where eID systems already exist but in which theses systems are restricted to certain regions or to a limited range of services, e.g. services by public administrations. This can go so far that a system can also be used for as a general ID means granting access to the workplace, the gym, the library, etc.
- **Higher usability is a core need as it will lead to higher numbers of use cases and users.** Especially in countries where citizens still need to be convinced to use eID-systems, user-friendly, secure and reliant systems like the IMPULSE-system could help to increase the number of users. Thus, all features contributing to user-friendliness of eID-systems like facial recognition for user identification, remote authentication combined with a high level of security are clear demands in the group of countries where eIDs already exist but are not used very heavily.

- **Access to e-gov-services, welfare services, banking etc. for citizens in fragile situations.** Similar to the situation in the Nordic countries, follower group it is also becoming an important need to provide access to different digital services to people with disabilities or people in fragile situations.

➢ **Latecomers**

The third group is latecomers which in our case is represented by Bulgaria. The purpose of the Bulgarian pilot was to explore if an eID solution could be implemented so that citizens could use it instead of other solutions (weak password, USB stick, etc.). As such, for the **Municipality of Peshtera (Bulgaria)** it was to allow the validation of an innovative and holistic blockchain-based GDPR-compliant eID management solution aiming at improving efficiency of services offered to citizens, as well as unify citizen's information to the different council services.

On a more general level, two needs can be highlighted in the group of latecomers:

- **Onboarding of customers of banks and insurances.** There is a crucial need for eID systems to provide access not only to e-government services but also to banking and insurance services. Integrating public and business services in the eID-system allows for an increase in trust and improves the attractiveness of the system.
- **Need for confidence-building measures**. It seems that trust is missing in public systems and the political system in general is lacking in countries that can be seen as latecomers. Even if there are e-government services available and back-office digitization is on track, people in these countries do not easily use the offer as people widely mistrust the state system in general. The need for trust in public authorities is crucial for the success of eID-systems but cannot be facilitated by eID-initiatives alone.

2.2.2 Requirements for the further adoption of the IMPULSE-solution

As we are interested in the further uptake and adoption of the IMPULSE-solution we have analysed the specific requirements for such an adoption in the different countries. In the following, the results will be presented for the three groups (leaders, followers and latecomers). The results are mainly drawn from the workshops documentation D6.2.

➢ **Leaders**

For leaders, the main requirements for further adoption of IMPULSE in their countries are:

- **Protection against cyberattacks**. Cyberattacks are a problem for eID-systems and their damage increases with more people use online-services. Thus, system security is a key requirement for the IMPULSE system as it is for any other eID-system or platform.
- **EU-regulations to allow for onboarding without having to check identities manually**. Currently, EU-regulation requires manual ID-checks for onboarding of users. This will be a challenge for the scaling up of any advanced eID system.
- **User-friendliness, ease of use and convincing procedure enabling all kinds of people to use the system.** This is a central requirement to be addressed when trying to introduce IMPULSE or parts of the IMPULSE system in leading countries with already working eID-systems. Path dependencies have to be considered. An entirely new system will be difficult to establish when there are already working ones, especially as service providers usually are reluctant to switch or to offer their service simultaneously on two different systems. Also, users may be confused if they have to use multiple eIDs.

- **Time to build up eID-infrastructures.** On a practical level, it is important to consider that building an eID-system and the respective infrastructures require a long process. Leading countries have made the experience that this a long process in which not only technical issues need to be solved but also the needs of users are to be aligned, standards are to be integrated and rules to be observed.

➢ **Followers**

In the group of the followers, the main requirements for the further adoption of IMPULSE are:

- **Clear advantages of the new system versus existing systems.** In countries where eID-systems already exist and are being promoted, a new system needs to show clear advantages compared to existing ones: The new system can be more user-friendly, more secure, allowing for more services, etc. In general, it is difficult to establish a second eID system like IMPULSE when people are already familiar with one. One option for IMPULSE is therefore to promote certain aspects like its ease of use, its high level of assurance, the SSI-approach giving users sovereignty over their data etc.
- **Communication of unique features of the IMPULSE-DLT/SSI-approach.** Not all users of eID-systems are familiar with the underlying technology and the features it allows. Thus, it is an important requirement for any strategy aiming at the implementation of IMPULSE in the group of followers to communicate and promote the advantages of the IMPULSE-approach using DLT/SSI-infrastructures.
- **Privacy and security of data stored need to be guaranteed.** The fear of surveillance and abuse of personal and especially biometric info has to be reckoned. Some citizens see eID-systems as instruments to control the population. A clear requirement here is to take these fears seriously and to focus on the information and communication of the advantages of the SSI-approach. A prerequisite for this is that the technical developments assuring privacy and security are finished accordingly.
- **Implementation of eIDAS 2.0.** Technology and service providers need planning security and Europe-wide standards. In the course of the implementation of eIDAS2, approved in November 2024, it is necessary that all systems have the same definition and implementation specification of the levels of security. Also, a *de facto* scheme for remote biometric enrolment needs to be agreed on. These are requirements that are principally important for all three groups (leaders, followers and latecomers). However, in the group of followers, they are of special importance because adoption opportunities for IMPULSE would be much higher in these countries.

➢ **Latecomers**

In the group of the latecomers, the main requirements for the further adoption of IMPULSE are:

- **Measures to increase trust in the system and in the political system as a whole.** Since the success of eID systems depends on the degree of trustworthiness, it is a key requirement to build and offer a system that people trust. As the development is largely coordinated by the state, it is particularly important in the latecomer-country under consideration here to build trust in the political system as a whole. Increasing political stability, however, is beyond the scope of IMPULSE's activities and is therefore an overriding requirement.
- **Focus on safety, fraud prevention and privacy.** If IMPULSE is to be adopted in the latecomer-country under consideration here, it needs to focus on aspects like safety, fraud prevention and privacy. This requires to successfully coordinate technical and legal aspects of the system.
- **Business use and e-gov shall be combined.** Another requirement for a possible introduction of IMPULSE in the group of latecomers is the integration of business applications (banks, insurances, e-commerce) into the system. E-government services alone will not be enough to make the system attractive, especially in countries where users are not yet familiar with an eID-system.

2.3 Intergroup similarities

In addition to group-specific needs and requirements there are some aspects that are equally important for all countries, be they leaders, followers or latecomers in terms of eID-availability and use. Similarities can be found on a general level (public administration services, integration of different services, acceptance, etc.) and on a concrete level addressing future tasks of the IMPULSE-provider if it is to be adopted in Europe.

The general similarities are:

- **Public administrations services:** Public administration services are increasingly allowing access via eID-systems. The transition of e-government services is a central prerequisite for the success of eID-systems. As soon as public administration services can be accessed online one way to promote their use is to make digital a standard, if not mandatory and provide analogue access only in exceptional cases.
- **Integration of different services:** The future adoption of IMPULSE requires to not only focus on public administration services but needs to integrate business solutions as well (banking, insurances, e-commerce).
- **Acceptance of the technology:** Both public administrations and citizens need to trust the system before they actually start to use it. IMPULSE with its Self-Sovereign Identity-approach can provide trust and confidence on a technical level. For future users it is important to inform about the SSI-approach and its implications for both legal entities and natural persons. Passing on that knowledge and making it understood is an important ongoing work by all the actors on this field.
- **Legislation:** The future adoption of IMPULSE in different countries also depends on an adequate implementation of eIDAS2. Europe-wide standards on implementations are central for eID-solutions to be offered across borders.

The specific similarities are:

- **Liaise with the DC4EU-project:** The European Commission has set a target of providing every citizen of the EU with a secure and user-friendly eID by 2030. Currently, there are four Large Scale Projects (LSRs) under way which are designed to develop technical solutions (toolboxes) and provide implementation know-how for a series of use cases. For IMPULSE, the next step on its way to a broader diffusion in Europe is to closely cooperate with these projects, especially with the DC4EU-project which also uses an SSI-approach.
- **Solve technical issues with impacts on trust and acceptance of IMPULSE:** One important challenge on the way to wider adoption is to find solutions on how to avoid false negatives and false positives in the identification process. Another challenge is to make the system secure against cyberattacks. And a third challenge is to allow for a fully automated onboarding process without a cross-check involving a real person. All three issues are of a technical nature but they nevertheless have consequences for the trust and acceptance of the IMPULSE-system.

3 Technological perspectives

3.1 Technological standpoint

3.1.1 IMPULSE solution

The IMPULSE User Wallet is contained in an Android mobile application, and it is responsible for storing and managing the user's verifiable credentials and associated cryptographic material. It offers the credential holder capabilities of a self-sovereign identity model, including the request for issuance of a verifiable credential, and the presentation of a verifiable credential. Additionally, and related to the issuance of the verifiable credential, the digital wallet, through its graphic interface, allows the user to perform the digital onboarding process that identifies their person prior to the issuance of their credential. Finally, this digital wallet can be integrated with a facial correlation module that will protect the verifiable credentials stored in the device, and with a service that will manage user consent on the correspondent privacy policies.

The IMPULSE Enterprise Digital Wallet is contained in a deployable service through a Docker container, and it is responsible for providing the functionalities of issuer and verifier of verifiable credentials to the corresponding public administration. Additionally, it offers a digital onboarding as a necessary mechanism for the correct identification of the person, prior to the issuance of their credential. Finally, this digital wallet can be integrated with a facial correlation service that verifies the correspondence between the faces of a selfie and a photograph of an identity document, with a document validation service capable of verifying that an identity document is authentic by analysing a photograph, and with a remote qSeal service capable of digitally signing verifiable credentials with a qualified signature.

- **Onboarding**

When citizen decide to use a certain public service online, they access it through their web browser. If it is the first time, they will be asked to go through a registration process via their digital wallet mobile application. First, the user's mobile app will obtain the DID Document and the legal entity URL directly from the EBSI blockchain to verify that the public administration is a trusted issuer. Once the citizen gives consent to share personal information, the mobile app asks them to upload photos of their face and ID document. Before sending the photos to the IMPULSE enterprise wallet, a biometric module integrated in the mobile application will register the biometric profile on the citizen's mobile device for further validations in the authentication process.

When the enterprise wallet receives both photos, selfie and ID document, it will invoke the corresponding AI services to perform a facial correlation between the selfie and the ID card to check if the person presenting the ID document is the real owner of it. It will then perform the document verification to validate that the presented document is authentic. This document verification service also reads the MRZ of the ID document image, information that will later be used to create the verifiable credential. Although the verification of the citizen's identity can be done fully automatically, in order to comply with the eIDAS regulation, a public servant will manually approve or reject the documentation (face and ID photos) provided by the citizen. If the verifications are successful, the corporate digital wallet will create the identity verifiable credential, invoke the remote stamping service to sign it with a qualified signature, and send it to the user asynchronously. At this point the user is successfully registered and can use their credential to access the online public service.

- **Authentication**

Once the citizen has been duly registered in the system, and consequently received an identity verifiable credential, they can authenticate with the online public administration service using their user wallet. First, the citizen accesses the public administration's web service via a browser using a PC/smartphone/tablet and clicks on the alternative login option (corresponding to the IMPULSE system). At this point, the public service

displays a QR code to be scanned with the mobile digital wallet, or a deep link that redirects to the user application. Then, the user wallet verifies the identity of the public administration by obtaining the public administration's information in EBSI, and requests the user to select the identity verifiable credential previously obtained. To protect the usage of this credential, the digital user wallet asks the person to take a selfie to compare it with the biometric profile previously created during registration, and thus unlock the verifiable identity credential. If the above steps are successful and the citizen gives consent to share their personal information, the user wallet makes a presentation of their identity verifiable credential to the public administration's enterprise wallet.

The enterprise wallet obtains the identity verifiable credential issuer's information directly from the EBSI blockchain and verifies whether it is a valid trusted issuer. After that, it verifies that the credential is authentic, and that the presentation of the credential is also valid. If everything is correctly verified, the user is authenticated and is able to consume the requested online public service in the browser of their PC / tablet / smartphone.

3.1.2 Biometric module and services

On the one hand there is the module focused on the facial identity verification between a user selfie and its ID document at the server side (Biometric Service in the PA domain). On the other hand, there is the module that allows users to get access to the ID-VC stored on mobile devices once they are registered in the platform (Biometric module in the User domain).

- **Server-side**: The server-side technology block (server block) is in charge of verifying user identity using its selfie and the portrait face photo available in its ID document. Furthermore, this block also carries out a presentation attack detection (PAD) analysis over the user's selfie to detect possible attempts of identity spoofing.
- **Mobile device**: The mobile device technology block (device block) enables the user to be authenticated locally after its registration in the IMPULSE platform. To achieve that, it exposes two main functionalities: 1. Face Profile Extraction: this functionality generates a user face profile from the user’s selfie also carrying out a PAD analysis similar to the server block does; and 2. Face Profiles comparison: this module is in charge of comparing two user face profiles giving a decision whether both face profiles belong to the same user or not.

In depth description of the building blocks of the artificial intelligence (AI) system, including the technologies used in each component, including their design, optimization, and evaluation:

- On the **server-side**, two main modules were developed: the Face Recognition module and the Face Presentation Attack Detection module.
- The **Face Recognition module** is designed to determine whether two images or videos belong to the same person. This module consists of four algorithmic blocks: Face Detection, Face Pre-processing, Feature Extraction, and Feature Matching.
- In the **Face Detection stage,** the Retina Face approach is used to find the location of the face within the image, and facial landmarks are produced for each detected face.
- In the **Face Pre-processing stage,** the face image is pre-processed to prepare it for the next stages, including aligning and scaling the face region to the canonical position and normalizing image pixels.
- In the **Feature Extraction stage**, a feature vector representing a face descriptor is produced using deep convolutional neural networks based on the Deep Residual Networks variant.
- Finally, in the **Feature Matching stage**, the face descriptors are compared using a cosine similarity function to determine if they belong to the same person.

To evaluate the security of the system, several evaluations were conducted on three different datasets: Labelled Faces in the Wild (LFW), IJB-C, and a private KYC Database.

- The **Face Presentation Attack Detection module** is designed to detect whether a user's selfie is a genuine presentation of the user or an impersonation attack attempting to mimic another identity. This module consists of three stages: Face Detection, Image Preprocessing, and Image Classifier.
- In the **Face Detection stage**, the same approach used for Face Recognition is used to check that there is a face present in the image to be processed.
- In the **Image Preprocessing stage**, the image is scaled to a common size and the pixels are normalized by centring their values at 0 and with minimum and maximum values belonging to the interval [-1, 1].
- In the **Image Classifier stage,** an image classifier is developed using Convolutional Neural Networks named EfficientNet, based on a dataset captured and annotated by ALICE.

In 2022/2023, the Face PAD algorithm was improved to make it more robust against real-world attacks by including a new attack type of mask attacks covering low-quality paper masks to high-quality silicone masks. The evaluation dataset consisted of 5067 samples from different identities. The improved algorithm's performance was compared to the previous system, and the results showed that the improved system had a higher true positive rate (TPR) at equal error rate (EER) and at false accept rate (FAR) of 1% for all attack types. The results obtained considering only OnScreen attacks, Printed attacks, Document ID attacks, and Mask attacks showed improvement over the previous system.

The algorithms used for the **mobile-side** are the same as those used for the server-side, except for the face recognition features extractor network architecture. A lighter network architecture called NASNet-A-Mobile was used due to the high resource consumption of neural network execution. The evaluation was carried out only on the IJB-C database, and the results show a true positive rate of 96.1% at EER, 89.8% at FAR=0.1%, and 82.9% at FAR=0.01%.

3.1.3 Document validation service

The purpose of this service is to assess whether a photograph of an ID document (ID card or passport) sent by a user of the IMPULSE solution corresponds to a genuine document (in other words, it has not been forged). This module is composed of three technology blocks:

- **MRZ code reader/validator:**

The MRZ code (machine-readable zone) encapsulates personal data and represent a security code which is included in all ID documents issued by European union member states. With the hashing mechanism being used in the MRZ codes, the integrity and security of the encoded data can be enhanced, helping to prevent fraud and tampering of identification documents. MRZ codes in passports generally consists of 2 lines × 44 characters. However, identity documents contain 3 lines of MRZ (30 characters each line).

We apply a state-of-the-art deep learning method based on LSTM (Long-short term memory) to detect word/sentence sequences on the ID document photograph. This library, Easyocr, allows to extract text with its corresponding bounding-box coordinates but also its respective confidence recognition rate (from 0 to 1). It is also combined with another OCR library, Pytesseract, operating on characters' level. This OCR tool recognizes text in different languages from all use cases ID documents (Bulgaria, Denmark, Spain Iceland, Italy).

To ensure the best conditions for users' experience during the onboarding process, the MRZ code reader endpoint returns all necessary data (name, surname, birthdate, ID document expiry date, etc.). So, data is automatically filled in the APP without the need to ask users to do this process manually. Should any correction be made, the user will be asked to update the form during the validation step.

- **Copy-move forgery detection:**

Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted on another part. In the context of ID documents, this forgery technique may be used to alter the image by reproducing some characters and respecting the utilized fonts and size. Hence, the objective of this verification component is to detect similar regions of the same image.

To achieve this goal, we extract all relevant key points and their corresponding descriptors using scale invariant fast transform method (SIFT). Since there are no objective reasons in manipulating fields of the ID document, using copy-move forgery technique, other than text fields, we will exclusively consider key points of the text fields zones. Then, we apply the density based spatial clustering applications with noise (DBSCAN) technique to identify similar key points inside text regions. The obtained clusters are potential copy-move forgery pairs.

- **Imitation forgery detection:**

Imitation forgery occurs when the font, size, colour, and any other morphologic characteristics of the text present on the ID documents is imitated, to introduce fake or manipulated data. Due to the available means, imitation forgery is always imperfect, leaving deviations in size, skewness and rotation with respect to the official text. This module aims to detect these traces left by the tampering process, thus obtaining evidence that the ID document is not legitimate.

Two OCR packages applying state-of-the-art techniques based on LSTM neural networks are used. This allows to extract the individual character images, from which features' vectors are built. These features' vectors are fed into a one-class SVM classifier which states whether the individual characters are in-class (genuine) or out-of-class (tampered). This classifier is built from a training set containing only examples of genuine ID documents and evaluated using a test set containing a balanced proportion of genuine and simulated tampered ID documents. The simulations have been produced by applying resizing, movement and rotation operations to an arbitrary subset of characters of genuine documents. The classifier output is aggregated as an ID document-level score, defined as the number of out-of-class characters within the document. From this score, the area under the ROC curve serves as the evaluation measure. In a production context, the module returns this score, which is used to calculate the global forgery score.

A forgery score is calculated based on the "*copy-move*" and the "*imitation*" forgery detection results. Depending on the document type and the nationality, a forgery threshold is also returned. This document-based threshold serves as a reference to decide whether the photograph is forged or not. Having the forgery score higher than the threshold means that photograph is manipulated, otherwise, it is considered as genuine.

Some auxiliary modules, necessary to the verification process, have also been developed, including: a quality image checker (if an image is dark or blurry), a cropping module and an OCR module employed to read the information present in the photographs.

- **Image quality check:**

The "*image quality check*" endpoint tests whether the image quality is sufficient to perform ID document forgery detection, or the end-user needs to upload a new photo. It is done by checking the level of brightness and sharpness of the provided image but also the confidence rate of the recognized text.

- **Cropping feature:**

To ensure good results when applying OCR techniques, the image/text must be in the good orientation. Furthermore, the photograph of the ID document must be cropped in a way to discard parts of the image that are not relevant and may interfere with to the verification task (e.g., background with text, fingers, etc.).

This automatic cropping method applies spatial invariant fast transform (SIFT) method to extract relevant key points and their corresponding descriptors. This is done for both images (reference image and the image we want to crop). Then, K nearest neighbour (KNN) method is applied to find matches between these two images. Finally, and after finding a minimum number of key points matches, a perspective transform is applied, and we obtain the cropped image.

In the second version of the API, we have disabled the cropping module for the interest of the user experience since a new feature has been added to the IMPULSE App by GRAD team. It consists in displaying frames during the photos capture process so, it helps final users to take the photos within these frames and then validate the resulting images or re-intent the process at their convenience.

- **Forgery proof image feature (explainable results):**

To rapidly interpret the forgery detection results and assist the public servant in his/her verification task, the verification module returns a forgery proof image. To explain the forgery verification results, straight lines with different colours link the origin and destination of copy-move forgeries. In case of morphological tampering, rectangles are surrounding the suspicious characters. Furthermore, a superimposed heatmap comes as an additional visual layer to stress the suspicious zones on the ID document.

3.1.4 Remote QSeal Services

This section describes the services dedicated to the signature and the validation of "Verifiable Credential" and "Verifiable Presentation" data structures. Services have been designed and realized following the guidelines and objects definitions contained in the EBSI related standards and in actual alignment with eIDAS technical guidelines. The validation engine in use is a specialisation of the CEF BB reference implementation. The report produced for the validation of JADES and JWS signatures will be in a proprietary format.

- **Service authentications**

The service is authenticated at two different level:

- REST resource: service REST resource are protected with an OAUTH2 Bearer token authentication. Tokens are generate using a direct password grant. Client id and client credentials are distributed to the service user by the Infocert Team.
- Signature is produced only if the issuer DID contained in the "to-be-signed" VC/CP matches the one contained in the certificate associated with the specific "user"

- **User enrolment**

To use the service users are required to comply with a lightweight "vetting procedure". The procedure is built to ascertain the identity of the requesting subject and his allowances before the completion of the onboarding. The main steps are:

- Vetting: Check subject's authorisations statuses vs EBSI TIR register
- Certificate issuance: generate the signature certificate from. Supported engine are:
    - Remote keys: certificate resides on a remote HSM (remote signature)
    - Software keys: certificate on a PKCS#12 keystore
        - Note that the PKCS12 objects must be configured server side to be used (WITHOUT the pin code, that is supplied by the user during the transaction)
- User enrollment: generation of the user/password needed to authenticate to the service and sharing of the client id and client credentials.

- **Service configuration**

Each user will need to request a specific activation server-side to enable/to change a specific signature engine or to gain access to the validation service. If needed. the user will be requested to share any subCA/RootCA/PublicKey involved in the validation of the signed objects produced by means of the engine in use. Each issuer will be identified uniquely by a pair composed by the "did:ebsi" and a redable name (the IssuerName).

- **Signature function**

Signature services are implemented using two opensource standard cryptographic libraries implementation:

- SD-DSS for JADES signature: https://github.com/esig/dss
- Nimbus JOSE + JWT for JWS signature: https://github.com/felx/nimbus-jose-jwt

- **Validation function**

The validation engine in use is a specialisation of the CEF BB reference implementation "sd-dss". For JWS signatures the engine is based on the same libraries used for the signature creation.

3.2 Possible barriers

In deliverable D2.13 we have already identified several barriers and challenges which are listed in table 3. These barriers are further examined in the next subsections.

Table 3: Barriers and challenges of technology adoption (extract from D2.13)

Barrier / Challenge	Explanation
Age difference	User's age can have an effect on how well they accept and adopt changes in their services.
Level of knowledge and education	The level of education will affect the users' knowledge, competence and willingness to try new things. Users with less knowledge may be more distrustful towards new services and technologies.
Previous experience	The previous experiences users have will have a positive or negative effect on how they perceive similar services and technologies.
Privacy concerns	Users have a varying level of privacy concerns. Some share personal information more willingly than others.
Security concerns	Users will have security concerns that need to be properly explained and shared with users.
Technical competency and available technology	Users have different levels of comfort and knowledge on how to use technology. Some have difficulties using new technology. In addition, not all users have smartphones, tablets, computers and other technology readily available.
Value vs. Required work	The service or technology needs to bring value to the user, and the value needs to be higher than the required work to be able to use the service.

3.2.1 Technological competencies

Each person has **different levels of technological competencies and available technologies** to be utilized (Keil et al., 2022[2]). Depending on their background and work, people might have several mobile devices, such as laptops, tablets, smartphones, and smart watches amongst other things. If a person has a high level of comfort and technological competency, they are more likely to have more and newer technological devices. On the other hand, there are people who have only few mobile devices that are much older and might not function with new digital services. In the worst case, people might be fully reliant on physical services as they have no functioning smart devices. Implementing an eID or digital solution in a scenario where not all users have access to a digital identity, can be detrimental for service adoption. It is vital to make sure that all people have equal opportunity to access the service, especially when it is a public service. Another limiting factor with some eID is the usage of facial recognition. There needs to be a functioning camera as well as the device itself needs to be able to support the technology and there might be people, who have an older smart device or a device where the camera is not functioning properly.

Another factor that can act as a barrier related to technological competency is the **value and required work ratio**. All users of a service use it because it brings some sort of value to them and everyone makes decisions based on how much effort they need to put in to achieve the value. If a service and the connected technology requires more effort than what it is valued at, the users will more likely decide not to use it. If users are given an option to choose between a physical or a digital service, they will use the one that brings them the best value compared to the effort needed. The value can be tangible, such as money or time, or intangible, such as ease of use or enjoyment. This means that any technology that is tied to a digital service, should be as convenient as

[2] Keil, M., Markert, P., & Dürmuth, M. (2022). "It's Just a Lot of Prerequisites": A User Perception and Usability Analysis of the German ID Card as a FIDO2 Authenticator. Proceedings of the 2022 European Symposium on Usable Security.

possible and bring the most value for users. In some cases, the service can be vital for users so they will end up using it regardless of how much effort is required (Andersen, 2021; Portz et al., 2019; Sohn & Kwon, 2020[3]).

The third factor that can be a barrier tied to technological competency are **previous experiences**. If users have experience with a specific technology, they will be more competent in the usage. Additionally, they will have a prejudiced perception based on if they have had good or bad experiences with a similar kind of technology. This means, that novel technologies may have inherent barriers as people are not familiar with them and do not know how they actually work. On the other hand, users may also be uncomfortable with a well-known technology if they have had bad experiences previously (Cubric, 2020[4]; Friedhoff et al., 2023[5]; Guggenberger et al., 2023[6]; Portz et al., 2019[7]).

Considering the six case locations within the IMPULSE project, these three different barriers can be seen on a varying level. For example, ARH and RVK have a nation-wide working eID scheme that most citizens are familiar with and know how to use. This means, that many public services are already offered in a digital form and ARH and RVK citizens already have previous experience in using eID technologies as well as increased technological competency and available technologies. All these will make it easier for them to adopt and accept a new eID technology entering the market. On the other hand, the citizens have some sort of baseline for value and effort -ratio, creating a larger barrier for newer entries to the marketspace as now they have to be able to provide better value with less effort. Similarly, UCIC has a widely used eID scheme though not at the same level as ARH and RVK and thus, UCIC will have similar positives and negatives.

Out of the case locations, MOP has the most limited eID scheme currently. Their digital identity revolves around the usage of a qualified electronic signature (QES) that requires a separate USB device and can only be used with a computer. This means that accessing digital services cannot be done with mobile devices, limiting the access quite heavily. Additionally, not all people even own the QES device and would rather use physical services unless forced to use a digital one.

In ERTZ, the current service is being provided in a digital form but the identification has to be done physically. Whenever a citizen has to submit a report to ERTZ, they can do so using the web platform but have to identify themselves at a police station within three days, making the use of a web platform slightly less encouraged. Having the option to fully identify online would help citizens and the employees to save time. In GIJON, the citizens have a physical citizen card they use to access services online. At the same time, the physical card gives additional functionalities to the citizens that cannot be done with just a digital identification, making the physical card more flexible and multipurpose. While they have an infrastructure that would support fully digital services, the physical card is still deemed necessary.

[3] Andersen, M.S. (2021). Towards the Design of a Privacy-preserving Attribute Based Credentials-based Digital ID in Denmark – Usefulness, Barriers, and Recommendations. Proceedings of the 16th International Conference on Availability, Reliability and Security.

[4] Cubric, M. (2020). Drivers, barriers and social considerations for AI adoption in business and management: A tertiary study. Technology in Society, 62, 101257.

[5] Friedhoff, T., Au, C., Ladnar, N., Stein, D., & Zureck, A. (2023). Analysis of Social Acceptance for the Use of Digital Identities. Comput., 12, 51.

[6] Guggenberger, T.M., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023). Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications. Hawaii International Conference on System Sciences.

[7] Portz, J.D., Bayliss, E.A., Bull, S.S., Boxer, R.S., Bekelman, D.B., Gleason, K.S., & Czaja, S.J. (2019). Using the Technology Acceptance Model to Explore User Experience, Intent to Use, and Use Behavior of a Patient Portal Among Older Adults With Multiple Chronic Conditions: Descriptive Qualitative Study. Journal of Medical Internet Research, 21.

3.2.2 e-literacy

There are two major factors that will affect the e-literacy of potential users that can act as barriers for technological adoption: **level of knowledge and education**. With a wider audience, users will have different levels of prior knowledge and education, making them a heterogenous group with different levels of skills to utilize digital and electronic material and tools. People with different demographic backgrounds, different ages, different communities and other variables will affect how e-literate they are. People with lower levels of knowledge and education will be less likely to first adopt a new technology or utilize a new service and would require more support, explanations and convincing (Cubric, 2020[8]; Friedhoff et al., 2023[9]; Guggenberger et al., 2023[10]). On the other hand, people with higher e-literacy levels may act as the pioneers for adopting new services and should be the first people to be targeted. To resolve these issues, the service providers need to consider that there are people who may be unwilling to immediately start using the new service and should have another method, such as physical, of providing the service (Friedhoff et al., 2023[11]).

In the six cases of the IMPULSE project, ARH, RVK and UCIC citizens all are quite adept users of technology. However, the current eID scheme in RVK has some accessibility issues, making physical services mandatory for those, who are somehow impaired. In ARH, some people prefer human interaction as an option compared to just fully digital services. On the other hand, citizens in MOP see their current digital services difficult to use and have a very low level of knowledge and skills. Thus, they would rather use physical services whenever possible.

The two Spanish cases are in the middle of the other cases. The people in ERTZ and GIJON have some level of knowledge on eIDs and have used digital services before but they also have a liking to physical services and would opt to either one depending on the situation. Especially in the case of GIJON, where they currently have a physical object, Gijon citizen card, that can be used to pay for bus rides in addition to signing in to digital services, the fully digital solution would have to somehow be able to replace the functionalities of the citizen card.

3.3 Implementation to the existing public administrations' services

Each of the different case locations in the IMPULSE project have their own existing digital identity solutions. While the implementation of the IMPULSE solution is similar in all cases, there are some major differences that have an impact on how the new service is implemented in the existing landscape.

While Denmark, and by extension ARH, has a working eID scheme, the case where the IMPULSE solution was implemented is a new partially digital service, instead of an existing one. The purpose was to have vulnerable citizens have access to lockers where they could store important documents and small items. The locker was tied to IMPULSE so that the users would be able to access their own locker after identifying themselves. A similar locker access could be provided with just giving out an SMS code to the user but that is not as secure but it would be easier to use. The full integration that was planned was only completed partially as the locker could not be fully connected to the IMPULSE solution. The lack of integration was only technical,

[8] Cubric, M. (2020). Drivers, barriers and social considerations for AI adoption in business and management: A tertiary study. Technology in Society, 62, 101257.
[9] Friedhoff, T., Au, C., Ladnar, N., Stein, D., & Zureck, A. (2023). Analysis of Social Acceptance for the Use of Digital Identities. Comput., 12, 51.
[10] Guggenberger, T.M., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023). Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications. Hawaii International Conference on System Sciences.
[11] Friedhoff, T., Au, C., Ladnar, N., Stein, D., & Zureck, A. (2023). Analysis of Social Acceptance for the Use of Digital Identities. Comput., 12, 51.

and it is assessed that the test users did not experience any difference in user experience, as there was only about a 1-second delay in their login with IMPULSE app and the opening of their personal draw, which were remotely opened. To further develop this service, the locker could have an integrated camera and it could have a stand-alone installation of the IMPULSE solution, removing the need for users to have a smartphone and they could use the locker with just an embedded user interface.

ERTZ infrastructure worked differently compared to the other cases. As the citizen did not require to login to the system, the IMPULSE solution now presented a new login layer that had to be differently integrated. In addition, there were other differences, such as the use of proxies, that required special care by modifying the Enterprise Service used with the IMPULSE solution, but the solution was properly integrated with the ERTZ digital platform.

GIJON currently provide citizens with a citizen card to be used to access digital services they provide. With the card, citizens are provided with online login details, such as a pin code, that they use to login. The IMPULSE solution would provide an alternative method of signing in to the services instead of using the code and pin numbers that are tied to the citizen card. Thus, the IMPULSE solution could replace the citizen card in the login functionality but there are other features the IMPULSE solution cannot be used for. One example is paying for the public transportation that can be done with the citizen card but not with the IMPULSE solution. Additionally, GIJON still requires citizens to have the card even if they would use the IMPULSE solution for signing in to the services. As GIJON suffered from a hacking incident previously to pilot testing round, their trust in technology was reduced and the IMPULSE solution was deployed and testes as a dummy service.

The existing eID scheme in MOP uses a separate device that is connected to a computer. This means that citizens cannot access digital services with mobile devices and would need to carry a separate device with them everywhere. The adoption rate of the QES service has been quite low and most people would prefer physical services. The IMPULSE solution would change the landscape quite drastically as now citizens would be able to use the services with their mobile devices and could identify themselves with just a smartphone. The IMPULSE solution while being quite new, would also bring a lot of value to the citizens of MOP. As MOP decided to create their own digital service from scratch, the IMPULSE solution was integrated with that.

With RVK, there were some problems with the integration. The original service where IMPULSE solution was supposed to be used, was discontinued and it was decided that the IMPULSE solution would be implemented on a dummy service for testing purposes. Considering the current landscape of RVK, they have a national eID that is used as a login layer for many different digital services. If IMPULSE solution would provide useful, it could be added as another login layer to be used instead of their current eID.

Italy has a national eID scheme that is currently being used with the UCIC system. As a private company dealing with a lot of important and private data, UCIC has strict security rules that needs to be adhered to before a solution can be used in their infrastructure. The IMPULSE solution was deployed on a cloud service, separate from the UCIC infrastructure for testing purposes. Additionally, the IMPULSE solution requires a little more information from the user compared to what their current login method requests.

3.4 Resolving needs and gaps

3.4.1 Resolving the issues for a smoother instantiation

When implementing the IMPULSE solution on the various public administration (PA) websites, the teams came up against a number of technical obstacles. By learning from these ways of getting around or eliminating obstacles, a list of "points of vigilance" has been drawn up:

- Select the most relevant decentralized identity model for the use cases of the solution (EBSI/ESSIF in our case).
- Design the different information flows that will take place in the solution (based on the previous selected decentralized identity model) and submit them to the team to ensure flows are visualised, understood and validated
- Pre-test the technical blocks to avoid malfunction.
- Test the solution with all the technical blocks integrated.
- Take account of possible changes and prepare a plan B
- Create documentation of facilitate the instantiation of the solution by a PA.
- Create documentation to facilitate the integration of the solution with a PA service.
- Reach for and use feedback of the solution to make necessary improvements.

This list of aspects to consider when implementing the IMPULSE-solution can also be instructive for the continuation of the solution in the future.

3.4.2 Providing solutions to meet pilots requirements

In the deliverable D2.1, relevant stakeholders were analysed at the beginning of the project. This analysis provided several general requirements that the IMPULSE solutions and IMPULSE(-like) solutions should fulfil. The requirements are listed in the table below.

Table 4: Requirements that IMPULSE(-like) solutions should fulfil

#	Categories	Criterion	Goal or description
1	1: Compliance to EU level regulations on eID 2: eID technology and interoperability	Cross-border interoperability / Mutual recognition	To what extent can the artifact be used by citizens of any other EU Member State, according to the eIDAS Regulation (EU) 910/2014
2	3: Software quality characteristics	Scalability	New users, institutions, or federations can be added without having performance losses
3	3: Software quality characteristics	Maintainability	How much effort is required over time to correct, improve, or adapt the artifact to changes in the environment
4	3: Software quality characteristics	Modifiability	How quickly and cost-effectively can the artifact be changed
5	3: Software quality characteristics	Flexibility	The ease with which the artifact can be adapted to use in different applications or environments than originally planned
6	3: Software quality characteristics	Reliability / Technical robustness	How prone to errors is the artifact
7	3: Software quality characteristics 4: Secure and trusted access 5: Usability, inclusivity, and user experience	Reproducibility / Predictability	To what extent the artifact consistently exhibits the same behavior or produces similar/predictable outputs when the process is repeated under the same conditions

#	Categories	Criterion	Goal or description
8	1: Compliance to EU level regulations on eID 3: Software quality characteristics 4: Secure and trusted access	Traceability / Auditability	To what extent the artifact data sets and processes are thoroughly documented, to revise prior decisions, fix current errors, or prevent future errors
9	4: Secure and trusted access	Resilience to attack / Security and fraud prevention	How well it is protected against fake, illegitimate, malicious, or unauthorized accounts and users
10	1: Compliance to EU level regulations on eID 4: Secure and trusted access 5: Usability, inclusivity, and user experience	Awareness of personal data	To what extent the artifact informs the user about the conditions for data collection and further uses of their data
11	1: Compliance to EU level regulations on eID 4: Secure and trusted access 5: Usability, inclusivity, and user experience	Control / Governance over personal data	To what extent can the user decide or influence the conditions for data collection and further uses of their data
12	4: Secure and trusted access 5 Usability, inclusivity, and user experience	Dialog	The presence of tools or applications aimed at collecting citizen input to public policy
13	4: Secure and trusted access 5: Usability, inclusivity, and user experience	Transparency / Understandability / Explainability	To what extent does the user know or understand the internal functioning of the artifact
14	3: Software quality characteristics 4: Secure and trusted access 5: Usability, inclusivity, and user experience	Effectiveness / Validity / Functionality	Performance-based, how well the artifact achieves the user tasks or requirements that it is supposed to comply with
15	5: Usability, inclusivity, and user experience	Efficiency / Productivity	Time- or resource-based, how long does it take to use the artifact, minimizing redundancy
16	5: Usability, inclusivity, and user experience	Utility / Usefulness / Perceived benefits	People find the artifact useful or beneficial
17	5: Usability, inclusivity, and user experience	Learnability / Speed of learning	How long does it take to learn how to use the artifact effortlessly
18	5: Usability, inclusivity, and user experience	Memorability / Retention	How well or how much do users remember about the artifact without need for relearning each time
19	5: Usability, inclusivity, and user experience	Findability	How easy is to find or discover the artifact
20	5: Usability, inclusivity, and user experience	Structure / Content / Aesthetics / Information design	How relevant, understandable, organized, and aesthetically pleasing is the information presented
21	5: Usability, inclusivity, and user experience	Feedback saliency	The extent to which the artifact provides clear and understandable status updates or information about the user's progress
22	5: Usability, inclusivity, and user experience	Emotion / Affect	What kind of affective reactions does the artifact invoke
23	5: Usability, inclusivity, and user experience	Accessibility	People with impairments can equally use the artifact with minimal or no obstacles
24	5: Usability, inclusivity, and user experience	Sociability / Community	Presence of policies and practices supporting how the members of the same community interact with the artifact

More information, resources and references can be found in D2.1 as well as in deliverables D2.5 and D2.8 that provide the requirement specifications, functional- and non-functional requirements for the IMPULSE solution in more technical detail.

The requirements paved way to the design and development of the IMPULSE solution and many of the requirements were fully implemented. These original requirements led to some design decisions that the

IMPULSE solution followed. One major decision was the use and selection of the decentralized identity model, based on the EBSI/ESSIF. This led to the design of different information flows within the solution based in the model and the use of multiple smaller technical blocks that will make up the solution. The technical blocks then had to be implemented, tested and integrated individually as well as when put together to form the IMPULSE solution. With the help of user testing, the solution was improved two times to create the final product. After the solution itself was developed, the technological team created documentation that can be used to integrate and deploy the solution on different platforms and services.

From the user side, there were different needs and gaps for each specific use-case. In the case of ARH, the aim was to be able to access the lockers with (or without) a mobile device and increase security through verification that would restrict unauthorized access. In a similar fashion, the verification was an important part for ERTZ and MOP. In the case of ERTZ, the plan was to have users verify themselves without having to physically be on-site and with MOP, the removal of the QES device was the main driving point for verification.

On the other hand, accessibility was an important gap for RVK as their current eID scheme has some restrictions on who can have a digital identity and who cannot. The IMPULSE solution was seen as a possible alternative that could be used even by people who would have some accessibility issues. For UCIC, the use of blockchain was intriguing and for GIJON, they wanted to have some way of reducing the number of forgotten pin codes and passwords that users request every year.

4 Ethical perspectives

4.1 Disruptive technologies and ethics

Identity is a complex construct that is historically intertwined with, from the one hand the need of control over the individual by the State, and on the other hand with people's rights and construction of a relational self. For an individual being tied to a certain identity may mean being able (or not) to access certain rights or privileges or to being excluded and discriminated against, but also to be identified as subjects of certain rights and/or obligations. The question of what approach to identity to choose is not ethically neutral, but inevitably impacts on fundamental moral aspects of human life such as autonomy, self-determination, and self-identification. Should the individual and his/her rights and autonomy be privileged when choosing an identity management system, or should the society and its need for control be elected as guiding principle? How much an individual can be considered accountable over his/her actions and how much anonymity and freedom can be favoured over public responsibility and liability? Should the concept of identity be flattened to its "administrative", factual characteristics (name, age, residence, etc) or should be expanded, to include also "attributes" that together concur to define the individual, like studies, work experience, affiliations, etc?

The point is that when an identity management system is designed, a choice is inevitably made to privilege some values over others: control over autonomy, or self-determination over full accountability and traceability.

In a landscape that sees on one extreme a centralized identity model, where everything is managed by some sort of central authority that grants and guarantees people's identities and on the other extreme a completely decentralized system, where no one detains control over the data and the identities of individuals, the IMPULSE project – in line with the EU approach – chooses to adopt a decentralized electronic identity solution based on the self-sovereign identity model.

In the self-sovereign identity model, the individual is the sole owner and controller of its credentials. He is in biunivocal connection with his data and cannot be separated from them. Given the fact that he naturally possesses an identity it is his natural right to have a digital one that is in biunivocal correspondence with the physical one. In this model the individual is unique and cannot have more than an identity, but the identity can have several attributes that may vary overtime. Regarding the identity management aspect, Sovereignty is the ability to share verified credentials preferring minimal data disclosure, where the individuals exercise their control over identity relevant private data.

Being this identity forcefully unique and indissolubly connected with the individual, it should also be portable and valid cross-borders, accompanying the individual through his entire life. Some immediate consequences of this approach would be making it easier for the individual to access online services across borders, to gain an enhanced freedom of movement and of work, to experience a more inclusive society, where equal rights of access to services is granted to everyone, to feel free and safe while accessing and using online services, because privacy and security are completely respected. These are in fact some of the inspiring principles of the EU digital wallet project and of the IMPULSE digital identity solution.

Adopting a value sensitive design approach, the IMPULSE project embeds these and other values (deriving from a structured consultation with the main stakeholders during some co-creation workshops held at the beginning of the project) in its solution "by design", building its identity management system on their foundations in this adopting technical solutions – like blockchain and smart contracts – that ensure and make it possible for these values to be incorporated by the system.

4.2 Consideration for ethics

In particular, it emerges the IMPULSE eID solution has the following ethically desirable characteristics:

- It is respectful of people's rights to privacy and to control over their personal data and of the principle of data minimisation (GDPR).
- It is a system that grants the user freedom as to what do and to whom disclose access to his/her personal data. Since it is not centralized, the user is also free to withdraw from the system without risks of his/her identity continuing to be stored and accessed.
- It is secure, minimizing the risks of identity theft and spoofing.
- It recognises that the identity of the person is not (only) a matter of administrative identification, that it includes numerous and complex attributes that may vary over time while the identity persists, and that identity is more than the sum of basic demographic and biometric data.
- It is inclusive, helping also people with disabilities or impairments or living in rural areas to access public services.
- It is transparent, as the blockchain nodes are fully inspectable and by means of specifically designed icons it makes fully understandable by the user what he/she is doing and the consents he/she is giving.
- It is interoperable with other eID management systems, granting to the users a system that fully works.
- It is reachable even when the user has not with him his/her physical id card or his/her account, as it relies only on biometric authentication for the log in, being in this way accessible from anywhere.
- Making identity persistent through the different services, it also promotes a stronger responsibility and accountability of the subject.
- Through its co-creative approach, it is respectful of the stakeholders' views and embeds them in the design of the technical solution.
- Finally, it enhances participation and engagement of citizens, making it easier for the people to contact and communicate with the public administration and to use services online.

These 2 sections are a brief summary of eID ethics implications, but more details of SSI eID solutions based on facial recognition user authentication, can be found in "*D3.1 EU relevant legal framework*", "*D3.3 IMPULSE method for ethical and legal assessment"* and "*D3.7 Recommendations on standards, ethical, legal and privacy issues*"

5 Stakeholders' acceptance and engagement

One subject that came up repeatedly throughout the project was that of acceptance of and commitment to a new digital identity solution such as the one proposed by IMPULSE: who to involve, when, for what and within what scope?

Two levels are distinguished:

- That for the testing phase (from procurement to testing) of the solution during the project.
- The post-project phase, i.e. the idea of getting people to adopt, or at least to give rise to the idea of adopting, the principles of the solution.

In a large-scale project, often stakeholder will have their own requirements and methods of engagement. The D7.11 provides a stakeholder mapping and identifies the different stakeholders. These are shown in Figure 4 below.

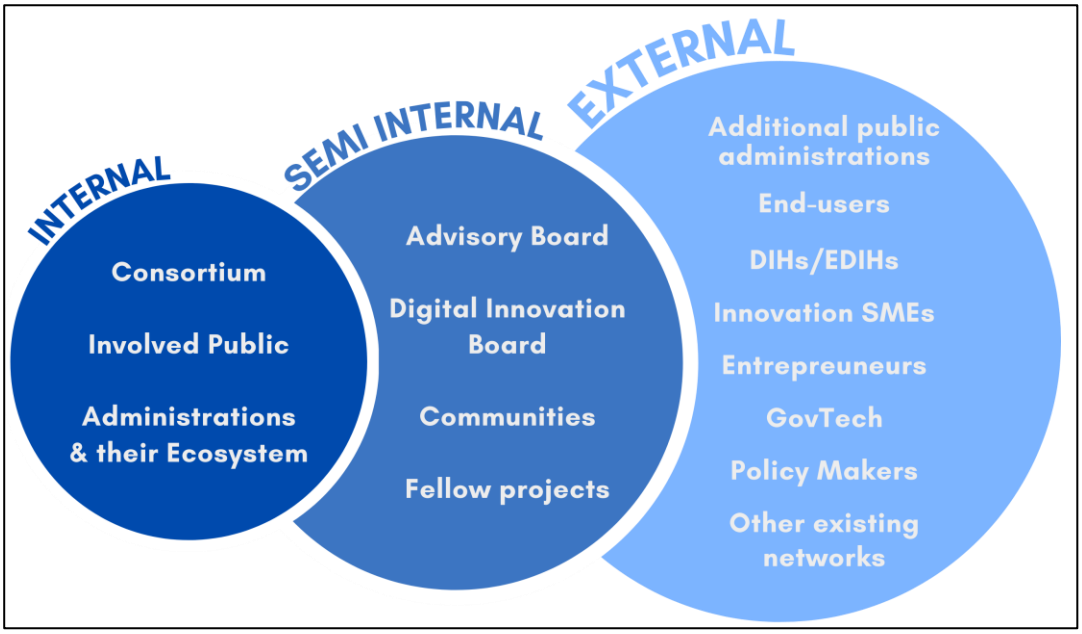


Figure 4 IMPULSE Stakeholders' list

Figure 4 shows sixteen different stakeholders involved in the project. The different stakeholders have been explained in more detail in D7.11. The involvement of the different stakeholders happenned during the project's lifetime and more than likely, the stakeholders were involved in multiple stages.

By internal stakeholders it is meant those who are directly and actively involved in the project. A distinction is made at mid-level of involvement for semi-internal stakeholders. These are the various partners or groups of interests who support the project but are not fully part of the consortium. External Stakeholders are individuals or groups outside a business or project, but who can affect or be affected by the business or project.

5.1 The upstream phase of implementing a digital solution

Based on the D2.13 (*Blueprints for enhanced public governance and public engagement*), there are five stages in the project development before the digital solution is launched and made available for the public:

1. Procurement stage

The procurement stage involves specific kind of stakeholders. Before the procurement stage, the citizens would voice their needs and requirements to direct the procurement of services and through the use of open forums, the public administrations could engage the citizens. As the service would be a long-term relationship, the service provider should be trustworthy. It is also important to consider the budget, security, ethics, data protection and other relevant aspects during the procurement stage. The procurement itself involves policy makers, PA ecosystem, PAs as well as entrepreneurs, GovTech, and innovative SMEs to discuss and provide possible options for purchasing the solutions and a working group that would support the project.

2. Design stage

The design stage involves many stakeholders as the most important aspect is to adopt a user-centric approach and involve all relevant users in the design process to be able to consider all possible scenarios and use cases. The stakeholders involved in the design team should develop user stories and there should be some kind of value being generated to the users that would be more than existing solutions. The value can be tangible or intangible as long as it is better than alternatives. These should also be considered during marketing and advertisement. Knowledge, views and information from experts and external advisors is highly valuable during the design stage.

3. Development stage

The development should follow ethical and legal standards and the development process should be transparent. During the development, the involvement of technical stakeholders, such as innovative SMEs and GovTech, will help to gain a better understanding on how would be best to go forward with the development process and how the end-users can be best accommodated, and their needs met. As with any good development cycle, there should be some form of testing involved during the development, and the different technical stakeholders can be involved in the internal testing phase (separate from the testing stage).

4. Instantiation stage

The instantiation stage is mainly the installation and setting up the solution to the platform for the service providers. This will involve the PAs and their ecosystem together with the developers of the solution. In addition, the policy makers need to be involved during this stage to ensure everything goes well and all relevant policies and procedures are followed.

5. Testing stage

The testing phase will involve stakeholders in a final test before the product would be implemented and launched. Stakeholders should be involved as much as possible with participants from different groups aside from just end-users, such as the DIB, communities, and fellow projects, to provide feedback from various perspectives. The participants in the testing could promote the solution to other people after launching as they have first-hand experience with the solution. During the testing, the developers should try to gather user interaction and feedback to improve the solution as much as possible before the final launch.

STAKEHOLDER	PROCUREMENT	DESIGN	DEVELOPMENT	INSTANTIATION	TESTING	OVERALL SUPPORT
CONSORTIUM	P	✓	✓	P	✓	
INVOLVED PA	✓	✓		P	✓	
PA ECOSYSTEM	✓		P	✓	✓	
ADVISORY BOARD		P			P	✓
DIB		✓			✓	✓
COMMUNITIES		P			✓	✓
FELLOW PROJECTS		P			✓	
ADDITIONAL PA		P			✓	✓
END USERS		✓			✓	
(E)DIH		✓			✓	✓
INNOVATIVE SME	✓	P	P	P		✓
ENTREPRENEURS	✓					
GOVTECH	✓		P	P	P	✓
POLICY MAKERS	✓	P	P	✓		✓
OTHER EXISTING NETWORKS		P			P	✓

Figure 5.5 Stakeholders' involvement by phase

The involvement of different stakeholders in each stage is recapped in the Figure 5. Check mark means that it requires full involvement from the stakeholder in the given stage and P means partial involvement. Partial involvement can be about having some contributions to the stage, such as the consortium only partially being involved in the instantiation phase (as mainly the technical consortium members are supporting the PA ecosystems but the whole consortium is not involved).

5.2 Key points for acceptance and engagement to a new solution

Overall, it is possible to draw up major factors that can influence the adoption and the success of an identity management system as the one being developed by IMPULSE:

- **Communication**

A strong and targeted communication campaign is of the utmost importance to ensure the successful adoption of any new identity management system. Different groups should be identified (especially the vulnerable ones, more at risk of un-acceptance) and ad-hoc communication actions should be delivered, making also use of unconventional techniques such as games, workshops, school labs, competitions, referral programs, etc. The key factors that make IMPULSE advantageous and different from other existing systems should be stressed out, underlining in particular the reasons why a self-sovereign approach could increase personal data protection and users' autonomy. A fully transparent approach should be adopted, clearly explaining the approach and the

underlying technologies in dedicated Q&As and making clear the role and the limits of the adoption of AI techniques inside IMPULSE, not hiding the risks but stating clearly the connected mitigation actions. The outcomes of the pilots should be periodically communicated, including the shortcomings and the identified solutions, making the entire process accessible and clear.

- **Access to services**

An attentive consideration of what services will be possible to access with a new identity management system is of the utmost importance. It emerged that the services you can access with the system could have a stronger effect on the outcome of the introduction of an eID system than the underlying technology: how enthralling the services are, or how essential they are for the citizen is an essential factor (for example many policy makers mentioned as killer services the EU Covid Certificate, the so called "Green Pass", or also the access to pension or to healthcare services). Citizens may not trust the underlying technology, but if they need it for an easier access to essential services, they may decide to try it anyway. For this reason, extending IMPULSE and other similar projects also to private services (for example private banking) could be a good idea, because people are more used to them and it is more frequent they use them in their daily lives.

- **Context factors**

The digital savviness of the population and of the public administration, the presence of an adequate infrastructure (basically access to fast internet connection and availability of devices) and the pristine presence of another, well introduced system of electronic identity are the main context factors that have been spotted as potentially high impact on the successful introduction of a novel eID system. To overcome them a thorough analysis of the context is necessary, in order to elicit targeted actions towards the main points that – country by country – could cause the unacceptance or the failure of the novel eID system. With respect to the public administration the importance of a gradual approach has been stressed out, adopting introduction paths that are tailored to the characteristics of each public administration. The digital divide too could be a strong adverse factor, both with respect to the public administration and to the citizens. Actions at government level should be undertaken to overcome this problem. If another electronic identity system already exists in a certain country, obviously the question of the interoperability takes the floor as the starring factor.

- **Usability**

Finally, great care should be put on making the system and the platform fully usable, also to fragile or with special needs categories of people, since one of the objectives of any such system, at least in the EU, is to develop an electronic identity management system that is fully inclusive and that allows the access to services, the engagement and the participation of all the citizens.

6 Beyond IMPULSE

6.1 eIDAS2

As the IMPULSE solution deals with eID technology, the main European legal frameworks of relevance are the GDPR 2016/679 and the eIDAS 910/2014. Where the former provides a wide-reaching discipline on the protection of personal data, the latter focus instead on the legal and technical aspects related to eID. It must be underlined that both these pieces of legislation are regulations, therefore directly applicable to all State Members of the EU (Art. 288, TFEU).

GDPR: It was enacted in 2016 and addresses the protection of personal data in the European Union. However, toady is a milestone in data protection and privacy also at the international level, influencing legal endeavours well beyond the EU space (e.g. the California Consumer Privacy Act). Its content is based on well-grounded principles of privacy and data protection. In particular, Art. 5 states that personal data must be:

- Processed in a lawful, fair and transparent manner;
- Collected for specified, explicit and legitimate purpose;
- Adequate, relevant and limited to what is necessary (‘data minimisation’);
- Accurate;
- Kept in a form which permits identification of data subject for no longer than necessary (‘data storage’);
- Processed in a manner that ensures appropriate security of the personal data;
- In accordance with the principle of accountability.

eIDAS: It came into force in 2014 and is the EU regulation on eID and Trust Services in the European Single Market. At the time of its drafting, the rising of eCommerce and eID systems was creating the necessity for a European-wide legal framework on the authentication of individuals. Coherently, eIDAS addresses the issue of interoperability of eID systems inside the EU and legally recognises a certain set of proofs of authentication (e.g. electronic seals, electronic signatures and timestamps). However, it must be highlighted that this legal text has a focus on centralised eID systems. As expressed in its Recital 2: *[eIDAS] seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.*

The IMPULSE solution has been developed in compliance with both the legal frameworks above mentioned. Other legal aspects that were taken into close consideration are related to the use of the **European Blockchain Services Infrastructure (EBSI)**. Still, while the Consortium has considered developing the IMPULSE solution on strong legal foundations - which we have described before - it wants also to keep an eye on the future. Indeed, it would be detrimental to develop an eID solution without taking into account also incoming legal novelties on the matter. Moreover, eIDAS 2 contains several key features that can be directly linked to the IMPULSE solution and were not present in eIDAS, such as focus on decentralised eID systems and blockchain.

eIDAS2, the updated European regulation on electronic identification and trust services, is expected to have a significant impact on projects like IMPULSE (Identity Management in PUbLic SErvices). The eIDAS2 approval offers several opportunities and challenges for IMPULSE:

- Enhanced Trust and Security: The IMPULSE solution follows a Self-Sovereign Identity (SSI) decentralized model, focusing on Public Administrations (PAs) of the European Union. This model, supported by a trusted blockchain framework and using Verifiable Credentials (VCs), aligns with the eIDAS2. framework, enhancing trust and security in identity management.
- Facilitating Cross-border Authentication: One of the goals of IMPULSE is to enable easier and more secure cross-border authentication. This is in line with eIDAS2's objective to facilitate cross-border electronic transactions and interactions within the EU. The alignment of IMPULSE with the eIDAS2 framework would enable more efficient and secure verification of identities across EU member states.
- Mobile App for Identity Management: IMPULSE uses a mobile app, which will help in identifying citizens during the authentication phase with Verifiable Credentials. These VCs are generated and managed in an SSI model and duly verified following the ESSIF framework. This approach is consistent with the eIDAS2 vision, where digital wallets and mobile applications play a central role in identity management.
- Compliance with Data Protection Standards: IMPULSE is GDPR-compliant, which is also a key aspect of eIDAS2. Ensuring compliance with data protection standards is crucial for gaining public trust and for the legal viability of such systems.
- Creating a Unified Digital Identity: eIDAS2's objective is to create a unified digital identity for EU citizens. IMPULSE, with its focus on digital identity in public services, can contribute significantly to this goal. The project's outcomes include holistic AI and DLT technology supporting GDPR-compliant eID to complement existing EU identity schemas.
- Facilitating Private Sector Integration: eIDAS2 aims to improve the integration of private sector use of digital identities, which could also benefit IMPULSE. By enabling secure and simplified interactions between citizens and various service providers, both in the public and private sectors, the IMPULSE solution greatly enhances the user experience and efficiency of services.
- Potential for Innovative Use Cases: The flexibility of eIDAS2, including the ability to define several credentials associated to specific identity attributes of the citizens, opens future opportunities for innovative use cases using IMPULSE. This could lead to more versatile and user-friendly services for citizens.
- Driving Digital Innovation: IMPULSE conducted a multidisciplinary impact analysis on the integration of DLTs and AI in eID. This aligns with eIDAS2's vision of driving innovation in digital identity and trust services within the EU.

In summary, eIDAS2 can significantly benefit and induce changes in the IMPULSE outcomes by enhancing security, enabling cross-border identity verification, ensuring GDPR compliance, facilitating private sector integration, and driving digital innovation in identity management within the EU.

6.2 Further development in the IMPULSE participating countries

6.2.1 Iceland

Taking the IMPULSE eID system further in Iceland rests on its potential to meet existing demands, more precisely, that the IMPULSE system can be relied upon for absolute proof of identify in order to be certified alongside other authentication options without compromising what is a well-established performance- and safety-critical operation and governance of issuing and operating eIDs independently of the services they unlock.

Currently, the official eID in Iceland is commonly obtained by visiting in person the offices of any bank, cell phone provider, the Auðkenni ldP or Registers Iceland. Around 97% of the eligible population has an active

eID, however, people have to obtain a new one if they lose or damage their phone. Since the state-owned Auðkenni began issuing the eID App (2021) in place of the eID on a SIM (introduced in 2013), a person who does not have an existing eID but has an Icelandic passport can set up an eID (onboard) by reading the facial biometrics directly from their passport's chip (using NFC capability on smartphones) and matching that with a live facial scan. The technological solution of reading biometrics directly from passport chips is considered very reliable, while taking a photo of passports is not. Also, the latest generation of passports is deliberately designed to make it almost impossible to capture a sharp image of the information page. For foreign businesses and persons who do not have an Icelandic national identification number, the challenge is verifying the origin and integrity of their official original identification with absolute certainty before issuing an eID. As it stands, the IMPULSE solution will first have to pass formal certification of its functional capabilities and compliance with a host of standards. Only then could it attempt an uptake as part of the Icelandic eID and eGov ecosystem, for instance, an alternative for those who prefer using facial recognition to log into services. Facial recognition has significant appeal, but another challenge then is ease-of-use compatibility with solutions like FaceID and, accordingly, being a realistic option, e.g., for people who have difficulties punching buttons and numbers.

6.2.2 Denmark

Between 80 and 90 percent of the Danish population currently use the MitID for e-government, e-health, online-banking and other e-business services. It is based on the central personal identification number which is common in Nordic countries, and which allows for a unique identification of citizens via a central, state-operated database. MiID provider is Nets. As found, implement IMPULSE with Nets or include something in MitID is not a viable approach. Instead, one could challenge the common public infrastructure and potentially incorporate IMPULSEthrough that. The advantage of the IMPULSE system is that future users can be activated to the system (onboarding) without having to show up in person at a public office. This applies to Danish citizens but also for foreigners or expats who do not have a central personal identification number. For foreigners and expats, concrete technical and administrative solutions still must be developed, however. IMPULSE can contribute its AI-based document identification and verification technology to support this development. Since there will be no central citizen registration system on a European level, authentication alternatives have to be found for non-Danish citizens. Another route for the diffusion of IMPULSE in Denmark is to install the system as a whole as a competitor to the existing MitID-system. In principle, this is possible, but it gives rise to the question, how many eID-systems are wanted and useful in Denmark.

6.2.3 Spain

In Spain, the challenges for the future diffusion of IMPULSE are of technical, regulatory, and strategic nature. The technical challenge is to develop and implement a solution for an automatic remote authentication without a manual cross-check. To implement such a solution, regulation plays an important role. It is expected that the translation of eIDAS2 into national contexts will take more time than expected. The strategic challenge for the future of IMPULSE in Spain relates to the question whether IMPULSE shall be set up as a separate system competing with existing eID systems or as an integral component within existing systems.

In Spain, the national eID-system is DNIe (Documento Nacional de Identidad electrónico). For authentication, citizens need to insert their ID-cards into a smart card reader. A mobile version with name „DNIe en el móvil" (DNIe on the mobile) is planned for roll-out in 2023. Also, there are the Cl@ve eID-system and several municipal and regional eID-systems in place in Spain.

For all these systems, users need to go to an office for a one-time authentication. The advantage of the IMPULSE-system is that the onboarding process could be done entirely remote. The challenge for IMPULSE is the integration into existing systems. Thus, as a next step, existing eID systems operators need to be

approached and convinced to include IMPULSE with its facial recognition authentication capability. It will be important not only to approach public bodies but also banks and other private businesses for cost sharing.

Another genuine feature of the IMPULSE-system is that it uses Distributed Ledger Technology (DLT) which has advantages compared to centralized systems. These advantages need to be clearly stated and widely communicated in order to convince stakeholders to switch their systems to DLT.

6.2.4 Italy

The main challenge for the diffusion of IMPULSE in Italy is the integration of parts of the system into already existing eID-systems. In Italy, there are two systems in use: CIE (Carta d'Identità Elettronica) and SPID (Sistema Pubblico di Identità Digitale). CIE uses the information stored on the chip of the Italian passport and SPID is issued by a consortium of identity providers which are authorized by the Italian Agenzia per l´Italia Digitale. Since October 2021, a SPID digital identity is needed to access tax, income and revenue services. It is planned to increasingly open public administration and e-government websites to the SPID system. To register for SPID, users need to show up at an office of one of the consortium members (most likely the postal office) and show their passport. Also, it is possible to register using the video ident method, where an employee of the issuing body and the user communicate via a digital conferencing tool. For identification purposes, Italian users applying for a SPID eID then need to pay a symbolic sum by bank transfer.

By adopting the IMPULSE facial recognition and document analysis system, the registration process could be made more user-friendly and efficient. For IMPULSE, this means to team up with the stakeholders of the current systems and convince them of the advantages of IMPULSE. One of the main tasks for IMPULSE advertisers is to convince stakeholders that the system is secure and can be trusted. One aspect of this is to explain where exactly the personal data is stored and how it is practically secured.

In Italy, the number of eID users as well as the number of use cases are growing steadily. A more user-friendly onboarding process and easy-to-use app could lead to a variety of new use cases for example granting access to the workplace, the library, the gym, etc. A successful roll-out requires taking into account the interests of public bodies as well as private companies.

To establish another system in addition to CIE and SPID does not seem to be feasible. Thus, future steps to disseminate IMPULSE should focus on the integration of its unique features into existing systems.

6.2.5 Bulgaria

In Bulgaria, the development and introduction of eIDs is at the beginning. There have been several attempts to introduce a nationwide system, but political instability has so far prevented them from succeeding. Current plans envisage the introduction of a Bulgarian eID on the basis of the new Bulgarian identity card, which is to be introduced at the end of 2023 and on which biometric data is stored digitally. However, there are two private eID-systems available in Bulgaria: B-Trust and Evotrust. For identification, both systems require a personal visit at one of the companies´ offices, for the mobile app, a video ident procedure is being offered. B-Trust and Evotrust can be used to identify users for online banking, digital tax declarations, and for digitally submitting documents to state and municipal authorities.

The user-friendliness of both systems could be increased by integrating the IMPULSE authentication method into the existing systems. However, in Bulgaria, it would also be conceivable to introduce the IMPULSE system as a separate system alongside the existing ones, because the development has just begun. In both cases, a close cooperation with banks, insurances, and other private businesses would be necessary as well as the integration of public administrations to provide e-government services on national and municipal levels.

Further technical developments of the IMPULSE-system would also be necessary in order to make IMPULSE secure against cyberattacks, solve security issues and to address deep fakes. In Bulgaria, issues of security, fraud-prevention and privacy are of high priority. Citizens have little trust in digital systems so far – a fact that needs to be addressed by further activities of IMPULSE in Bulgaria.

Another challenge is to make clear to decision makers and future users that IMPULSE is not an identity provider but a technical system. The advantages of IMPULSE being a Self-Sovereign Identity (SSI) solution need to be clearly communicated. The future activities can be based on the experiences gained in the pilot carried out in the municipality of Pesthera.

6.2.6 What about IMPULSE in Europe

From the outset, the aim of the IMPULSE project was to develop an eID solution that could be used all over Europe. The main advantages of the IMPULSE-system are the facial recognition technology, the AI-based document analysis and the SSI-approach. The challenge is currently that there are many different systems and technical approaches used in European countries and even in different regions.

At national levels, the IMPULSE solution thus has to compete against existing systems or it has to cooperate with existing eID providers to integrate components of IMPULSE into these systems. At the European level, IMPULSE must strive to incorporate the technical solutions developed in the project into the standardization process and the so-called technical toolboxes.

The European Commission has set the a target of providing every citizen of the EU with a secure and user-friendly eID by 2030. Currently, there are four Large Scale Projects (LSRs) under way which are designed to develop technical solutions (toolboxes) and provide implementation know-how for a series of use cases. For IMPULSE, the next step on its way to a broader diffusion in Europe is to contact and cooperate with these projects, especially with the DC4EU-project which also uses an SSI-approach.

At the same time, the technical maturity of the IMPULSE needs to be developed further. During further development, care must be taken to ensure that the IMPULSE solution achieves a which is a requirement for all future European IDs. This includes to ensure a “high” level of assurance, an onboarding mechanism without a manual cross-check, a solution for false negatives, a safeguard against deep fakes, and a secure element solution which includes iPhone from Apple. Technical developments like these need to be aligned with eIDAS 2.0 and EUID wallet specifications. This is a significant but promising challenge as seen in the previous part.

Furthermore, public administrations as well as private companies have a role in the future dissemination of eID systems in general and the IMPULSE solution in particular: Public administrations need to further integrate eID-systems into their e-government ecosystems and securely link their systems to citizens´ eIDs, and private businesses need to further increase the number of services in which eIDs are used to identify users and customers.

7 Conclusions

This deliverable is the full analytical report for the WP6 that offers more details and descriptions to the 6+1 roadmaps developed within the work package. The roadmaps are meant to be easy to read and as concise as possible, which is why this analytical report will hold all the additional information. This analytical report combines information from the various other work packages as their input has been necessary for developing the roadmaps as well as to provide additional analytical details:

- WP2 provides the end-user analysis, pilot results, and blueprint for enhancing engagement as well as some of the technical details in relation to the overall architecture of the IMPULSE solution.
- WP3 provides the ethical and legal findings necessary to be considered when adopting and developing a new digital service
- WP5 provides more detailed technical information specifically to each technological component within the IMPULSE solution in comparison to the WP2 that provides more of a general overview.
- WP6 provides the workshops results arranged with external experts and public administrations that give further insight to the organizational processes of adopting and maintaining digital services as well as their expert views and opinions on electronic identity solutions

This report has a similar structure as the roadmaps to allow reader to use this document in conjunction with the roadmaps. Similar situations, barriers and recommendations presented in the roadmaps are described in this document, providing further details and analysis.

References

[1] E-government activities of individuals via websites, Online data code: isoc_ciegi_ac, DOI:0.2908/isoc_ciegi_ac – last update: 17/01/2024 23:00. https://ec.europa.eu/eurostat/databrowser/view/isoc_ciegi_ac__custom_9216875/default/table?lang=en

[2] Identification procedures used for online services (2020 onwards), Online data code: isoc_cisci_ip20. DOI: 10.2908/isoc_cisci_ip20 – Last update: 17/01/2024 23:00. https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_ip20__custom_9187977/default/table?lang=en

[3] *Countries' performance in digitisation*. (n.d.). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

[4] OECD (2022), Digital Transformation Maturity Model, OECD, Paris**.** www.oecd.org/tax/forum-on-tax-administration/publications-and-products/digital-transformation-maturity-model.htm

[5] Andersen, M.S. (2021). Towards the Design of a Privacy-preserving Attribute Based Credentials-based Digital ID in Denmark – Usefulness, Barriers, and Recommendations. *Proceedings of the 16th International Conference on Availability, Reliability and Security*.

[6] Cubric, M. (2020). Drivers, barriers and social considerations for AI adoption in business and management: A tertiary study. *Technology in Society*, *62*, 101257.

[7] Friedhoff, T., Au, C., Ladnar, N., Stein, D., & Zureck, A. (2023). Analysis of Social Acceptance for the Use of Digital Identities. *Comput.*, *12*, 51.

[8] Guggenberger, T.M., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023). Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications. *Hawaii International Conference on System Sciences*.

[9] Keil, M., Markert, P., & Dürmuth, M. (2022). "It's Just a Lot of Prerequisites": A User Perception and Usability Analysis of the German ID Card as a FIDO2 Authenticator. *Proceedings of the 2022 European Symposium on Usable Security*.

[10] Portz, J.D., Bayliss, E.A., Bull, S.S., Boxer, R.S., Bekelman, D.B., Gleason, K.S., & Czaja, S.J. (2019). Using the Technology Acceptance Model to Explore User Experience, Intent to Use, and Use Behavior of a Patient Portal Among Older Adults With Multiple Chronic Conditions: Descriptive Qualitative Study. *Journal of Medical Internet Research, 21*.

[11] Sohn, K., & Kwon, O. (2020). Technology acceptance theories and factors influencing artificial Intelligence-based intelligent products. *Telematics Informatics, 47*, 101324.