Impulse

Identity Management in PUbLic SErvices

D3.7 Recommendations on standards, ethical, legal and privacy issues

Lead Author: [Francesca Morpurgo (CEL), Tetiana Vasylieva (CEL), Lorenzo Maria Ratto Vaquer (CEL), Luca Mattei (CEL), Renè Lindner (DIN)]
With contributions from: [Carmela Occhipinti (CEL), Luigi Briguglio (CEL), Lorena Volpini (CEL)]
Reviewer: [Nicholas Martin (FhISI – Georgi Simeonov MOP]

Deliverable nature:	<Report (R) >
Dissemination level: (Confidentiality)	<Public (PU)>
Delivery date:	31-01-2024
Version:	1
Total number of pages:	55
Keywords:	Digital identity, eIDAS, EUDI wallet, eIDAS, Social acceptance, Ethics by design, Policy recommendations

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

Executive summary

This conclusive deliverable encapsulates discoveries and recommendations stemming from the IMPULSE project, catering to individuals and projects in allied domains, with a pronounced emphasis on policymakers and a diverse array of stakeholders. Beyond the realm of digital identity, it explores critical spheres such as innovation, change management in public services, technology acceptance, and the intricate interplay of regulatory factors with technological innovation. Additionally, it delves into the far-reaching societal impacts engendered by decisions made during the implementation of digital identity.

This document serves as a comprehensive compilation, synthesizing diverse aspects of the project to present a holistic perspective. It provides relevant information, recommendations, and lessons learned, categorizing main recommendations into ethics and legal, socio-economic, and standards. These categories, further nuanced by sub-categories, encompass factors like awareness, transparency, self-sovereignty, trust, and the distinctive impact of the IMPULSE solution on digital identity. This methodical approach aims to address key issues in a nuanced and exhaustive manner.

Recognising the crucial role of stakeholders, section 3 underscores the necessity of clearly defining them. Leveraging scholars' perspectives on stakeholders, it illuminates the diverse categories of individuals involved. The IMPULSE project's stakeholder analysis, employing established definitions, is meticulously detailed in tables, categorizing stakeholders based on functional, financial, political, and other roles. The document acknowledges broad and specific categorizations, clarifying its primary focus on the demand category while intermittently exploring governance and supply stakeholders. To augment reader engagement and flexibility, the document commits to linking recommendations and lessons learned to relevant stakeholder categories.

In section 4, delving into the concept of disruption, the document clarifies the need for a clear understanding within the context of the IMPULSE project. Drawing from Christensen's definition of disruptive technology, it underscores the potential for fundamental changes in technology, business models, and societal rules. The distinction between first-order and second-order disruptions is explored, positioning the IMPULSE eID solution more in alignment with the latter, accentuating its profound societal impacts over technological disruptiveness.

The document accentuates the regulatory framework's significance in implementing a digital identity system and acknowledges potential disruptive impacts. The IMPULSE project concentrates on identifying barriers to successful implementation, categorizing them into organizational, interaction-specific, innovation characteristics-related, contextual, and process stage-related barriers. The document delineates various barriers and proposes mitigation actions related to the implementation of a digital identity system.

Section 5 scrutinizes potential barriers and risks linked to the implementation of a digital identity system, specifically within the IMPULSE project. The barriers are methodically categorized into six types: organizational, interaction-specific, innovation characteristics-related, contextual, and process stage-related. Furthermore, it furnishes specific barriers discussed alongside mitigation actions.

Section 6, titled "Recommendations and Lessons Learned," reflects on key insights derived from the IMPULSE project, centring on ethical and legal facets, socio-economic issues, and standards pertaining to the introduction of an electronic identity (eID) system. The discussion encompasses the transformative impact of disruptive technologies, the project's stakeholders, and the primary barriers faced by eID projects. Special emphasis is placed on the ethical and legal considerations surrounding the Self-Sovereign Identity (SSI) approach adopted by IMPULSE.

Finally, the document concludes by summarizing findings and outlining potential avenues for future research.

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**	D3.7	**Title**	Recommendations on standards, ethical, legal and privacy issues
Work package	**Number**	WP3	**Title**	Multidisciplinary analysis of standards, legal and ethical implications
Task	**Number**	T3.5	**Title**	IMPULSE policy recommendations

Date of delivery	**Contractual**	M36	**Actual**	M36
Status	version 1.0		☒Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)				
Responsible author	**Name**	Francesca Morpurgo, Luca Mattei, Tetiana Vasylieva, Lorenzo Maria Ratto Vaquer, Renè Lindner		
	Partner	CEL, DIN	**E-mail**	f.morpurgo@cyberethicslab.com

Summary (for dissemination)	*Recommendations arising from the IMPULSE method for the implementation of disruptive technologies in the field of eID management for public services, and potential extension to other fields*
Keywords	*Digital identity, eIDAS, EUDI wallet, eIDAS, Social acceptance, Ethics by design, Policy recommendations*

Version Log			
2023/11/08	01	Francesca Morpurgo	First version of TOC
2023/11/15	02	Francesca Morpurgo	TOC discussed with partners and shared in the repository
2023/12/01	03	Francesca Morpurgo, Tetiana Vasylieva, Luca Mattei, Lorenzo Maria Ratto Vaquer	First draft
2023/12/18	04	Renè Lindner	Added section 6.3
2023/12/20	05	Francesca Morpurgo, Tetiana Vasylieva, Luca Mattei, Lorenzo Maria Ratto Vaquer	Second refined draft, expanded sections 5 and 6
2024/01/4	06	Francesca Morpurgo, Tetiana Vasylieva, Luca Mattei, Lorenzo Maria Ratto Vaquer, Lorena Volpini	Furtherly expanded all the sections, first internal revision
2024/01/8	07	Carmela Occhipinti, Luigi Briguglio	Second internal revision
2024/01/11	08	Francesca Morpurgo, Lorenzo Maria Ratto Vaquer	Final version
2024/01/26	**09**	Nicholas Martin, Georgi Simeonov	Internal revision
2024/01/31	10	Francesca Morpurgo	Final version

Table of contents

List of figures

List of tables

Abbreviations and acronyms

AD: Adequacy Decision
CJEU: Court of Justice of the European Union
CON: Contextual Barrier
DEC: Decision-makers Stakeholder
DEV: Developers Stakeholder
eID: Electronic identification
eIDAS: Electronic Identification, Authentication and trust Services (Regulation)
EUDIW: European Digital Identity Wallet
EXP: Advisors and Experts Stakeholder
FIN: Financial Stakeholder
FUN: Functional Stakeholder
GDPR: General Data Protection Regulation
HIR: Hired Consultants Stakeholder
ICT: Information and Communication Technologies
INT: Interaction specific Barriers
INN: Innovation characteristics related barriers
LoA: Levels of Assurance
NEG: Negatives Stakeholder
ORG: Organizational Barriers
OPE: Operators Stakeholder
PEST: Political, economic, social, and technological (analysis)
POL: Political Stakeholder
PRO: Barriers related to process stage
RES: Responsibles Stakeholder
REG: Regulators and Policymakers Stakeholder
SCCs: Standard Contractual Clauses
SPO: Sponsors Stakeholder
SSI: Self-Sovereign Identity

1 Introduction

IMPULSE is a very complex project, putting together many different experiences and competences that all converge towards the development and the assessment of a product that is at the same time a piece of software and an experiment about digital identity and digital wallets. Having adopted a bottom up, co-creative approach, since the beginning IMPULSE worked with a community of stakeholders, that have been continuously consulted throughout the lifespan of the project. This, together with the experience gained by all participants in delivering their contributions to the project, **makes IMPULSE a precious source of knowledge and experience for all those working in the same field**, whether they have to act as policy makers (e.g. they have to decide whether to invest or not into a certain project, or how to support it) or as project managers and/or developers (e.g. they have to understand what could be the better design choices and what could be dead ends). In this deliverable some hints regarding ethical and legal concerns, socio-economic issues and standards gained during the course of the project will be systematically reviewed and made available. The focus is in particular on what concerns the adoption and the acceptance of eID solutions as well as their ethical and societal impacts.

Since no technological solutions are aimed at everyone but rather each one targets a well definite set of stakeholders, the approach that here will be followed is to cascading first **the identification of the main stakeholders of the project, then the definition of disruptive technologies and the main barriers identified so far, and finally the recommendations and lessons learnt, divided by legal-ethical, socio-economic, and standards**.

In particular, since the IMPULSE project has the explicit aim of exploring the use and the introduction of disruptive technologies into digital identity management and public services, first of all a definition of the meaning of disruptive technologies is attempted, so that the application scope of the present deliverable and of the resulting recommendations is perfectly delimited. The focal point here is understanding what is impacted by the changes and innovations that the IMPULSE project deals with: technology, processes, ways of designing and implementing social changes, cross fertilization between regulatory and technological aspects… IMPULSE touches all these aspects and in the present deliverable it will be attempted an analysis of the boundaries of the impact of a similar approach and of the consequences in term of recommendations that can be derived from it.

The evidences that will be used in the present deliverable derive mainly from internal activities of the project but also relevant scientific literature will be examined and considered.

In particular, materials and recommendations will be extracted from the following work packages and deliverables:

- From the work package 2 (Co-creative design and piloting) evidence will be gathered from the pilot outcomes as compared with the initial co-creation workshops and from the blueprints for a successful development and implementation of an eID solution (deliverable D2.13)
- From the work package 3 (Multidisciplinary analysis of standards, legal and ethical implications) the insights that emerged during the two policy round tables will be exploited as well as the method for the ethical evaluation set up in the deliverable D3.3 ("IMPULSE method for ethical and legal assessment")
- From the work package 4 (Socio-economic/political impact analysis) the findings of the survey conducted within the context of the deliverable D4.2 and of the socio-economic analysis done in the D4.4 and D4.5 will add many useful insights
- From the work package 6 (Roadmapping for adoption, escalation and sustainability) the results of the country workshops will be particularly valuable (available in the deliverable D6.2) as they will shed light on the point of views and also on the recommendations coming from representatives from the different use cases countries.
- Finally, the findings of the PEST analysis and of the market research and of the exploitation plan, made in the context of the work package 7 - Innovation and exploitation management, dissemination and communication (deliverables D7.3 and D7.8) will be used to understand how external factors could combine and reinforce and/or mitigate the factors detected during the internal workshops and surveys.

Aiming at building a logical architecture this deliverable starts with an examination of the project's stakeholders, in the conviction that it is not possible to think of recommendations and lessons learnt without first establishing who is the receiver. In other words, it is crucial to understand who they are addressed to and for whom they can be of relevance. A very broad outline of any eID solution stakeholders is proposed, following the approach of (Lukkien, 2023). Then, the IMPULSE's stakeholders list is presented and a quick paragraph is dedicated to whether the two lists are compatible (section 3). Moreover, the concept of disruptive technologies is analysed to clarify the landscape and the broader scope of the IMPULSE project that has at its core the use and the adoption of disruptive technologies for its eID solution (section 4). In this context, it is argued that within a project dedicated to developing an eID solution not only technologies should be considered disruptive but also other factors, such as the regulative framework, whose transformative impact on the way digital identity is conceived and managed is assessed (section 4.2). Once the stakeholders' list has been defined and the concept of disruptiveness has been clarified, the text moves on to identify the potential barriers and risks that the introduction of any eID solution and of the IMPULSE one in particular has to face. The aim is to be able in the next sections to connect and mitigate them with the recommendations, that in this light will necessarily appear as actions to break down or at least mitigate the aforementioned barriers (section 5). Of course, the barriers and risks will be connected to the stakeholders' list, so as to clarify that each barrier is such only in relation to certain stakeholders and so to certain needs and certain contexts. First, following the approach of (Cinar, Trott, & Simms, 2019) a very general categorization of barriers is given, then a list of specific barriers, emerged during the development of the IMPULSE project, is attempted. Finally, in the section 6, some conclusions are drawn in the form of recommendations that can be derived from the work done during the project, coming both from the advice of external experts and from findings and reflections done by the project researchers and during the project's pilots. In this regard, the ethical, legal, social, economic and standardisation aspects are taken into account, and recommendations concerning each macro area are listed and briefly explained.

2 Why this deliverable and general approach

Coming at the end of the project, this deliverable must be thought of as a series of findings that may be useful for people or projects working in the same field. In particular policy makers, but also other stakeholders, as listed in the table 2 below.

This in turn involves much broader subject areas that the sole digital identity: innovation and change management in public services, acceptance of technology, the influence of regulatory aspects on technological innovation, the nature of identity and how deciding for a way or another of implementing it when it comes to digital identity shapes the society and the individuals, the main barriers and risks that can underlie any such project and its effects on the relationship between citizens and the state (Pierucci & Cesaroni, 2023).

During a project, many interesting aspects related with the project's central objectives and outcomes emerge, but they are often scattered, dispersed in several work groups. **This deliverable offers an opportunity to have a more general and holistic view and understanding and to extract and make quickly available the most relevant information and recommendations, as well as the lessons learned**.

As mentioned in the introduction, the most relevant findings from the main project deliverables will be used as a basis to formulate recommendations and lessons learnt and will be used as hints to trigger – in the present deliverable – further reflections.

To facilitate the orienteering inside the document, the main recommendations will be listed under three main categories: ethics and legal, socio-economic, and standards. Furtherly, they are sub-categorized adopting whenever possible the approach stated in the Description of Action (DoA), namely taking into account factors such as awareness, transparency, self-sovereignty, trust and impact of the IMPULSE solution, and in general of any digital identity solution, aiming thus to offer a proper view of the main issues to be addressed.

3 Stakeholders identification and list

Stakeholder may be an extremely broad term when used for everyone who may have an interest in a certain project or activity. Or, it can be extremely restricted, if used for identifying certain particular categories of people which the project intends to address. In any case, when drawing up recommendations it is extremely important that a special focus is dedicated to clarifying who these recommendations are addressing, so that it is possible to refine and customize them in order to make them truly effective.

(Lukkien, 2023) presents a list of stakeholders of the EUDI Wallet ecosystem, on its turn derived from the Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework (European Commission, 2023) and that is reported in the image 1 below and in the table 1

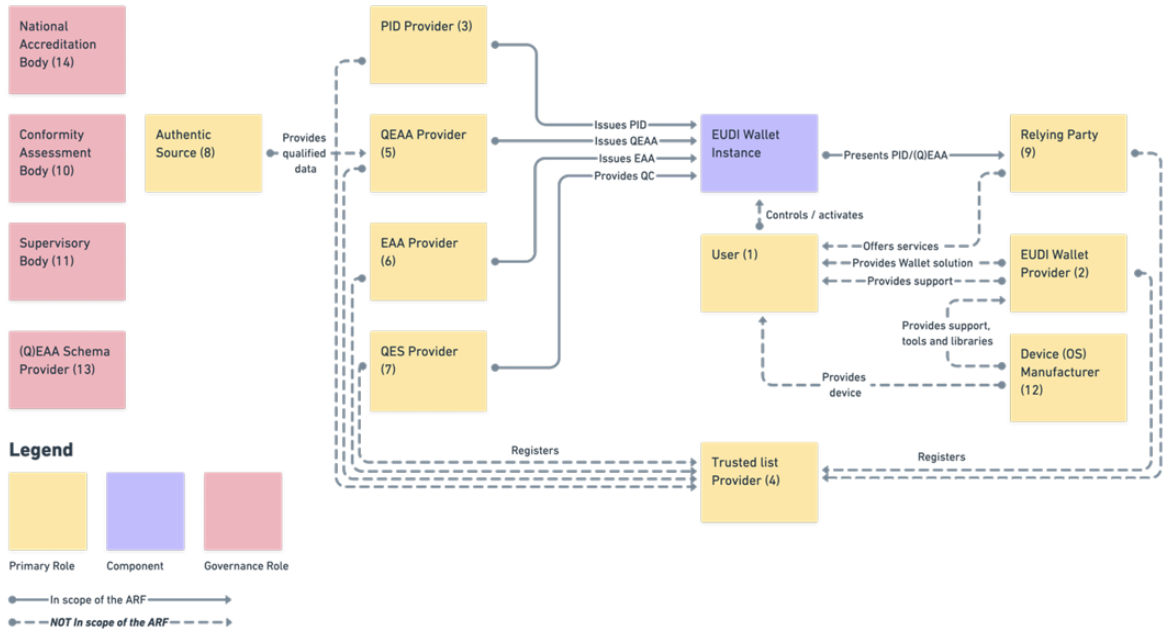


Figure 1 - stakeholders list from the Common Union Toolbox

Table 1: stakeholders list from Lukkien (2023)

Governance: 1. National accreditation bodies 2. National supervisory bodies	
Supply: 1. Identity provider (eIDAS schemes) 2. Attribute providers (eIDAS schemes) 3. Qualified trust service provider 4. Non-qualified trust service provider 5. Identity provider (non eIDAS schemes) 6. Attribute provider (non eIDAS schemes) 7. Technology providers 8. Conformity assessment bodies	Demand: 1. Citizens 2. Business 3. Public administration And 1. Public wallet service provider 2. Private wallet service provider 3. Public trust service provider 4. Online service providers (not eIDAS)

From this analysis, it is evident that the stakeholders to be considered inside any project addressing the matters of digital identity and its introduction are very diverse and with different needs and roles. In the context of the present deliverable, the approach of the deliverable D2.1 will be followed. Thus, a stakeholder is "any group or individual who can affect or is affected by the achievement of [the IMPULSE project] objectives" (Mitchell, 1997).

At the very beginning of the project, IMPULSE consortium identified (cf. WP2, deliverable D2.1) the categories of people who fall under the aforementioned definition, following in this already existing requirements deriving from engineering literature (Ballejos, 2008).

The results of this preliminary analysis are in the following table (source: IMPULSE project, deliverable D2.1).

Table 2: IMPULSE stakeholders list

Stakeholder Role	Description
Functional (Regular users or citizens)	Those who benefit directly from the functions or tasks performed by the system and its results. Citizens and service providers are likely to fall inside this category, because the implemented functionalities are beneficial to them.
Financial	Those who benefit indirectly from the system, by obtaining financial rewards, e.g.: funders, investors, representatives of mixed capital companies or public-private partnerships.
Political	Those who benefit indirectly from the system, by obtaining political gains in terms of power, influence, and/or prestige. Elected members of the local city councils and public administrations may be included here (unlike career civil servants who might not obtain political gains from the project and just oversee its execution).
Sponsors	Those in charge of facilitating and enabling the system development, by collecting funds and/or protecting them (e.g., against political pressures and budget reductions).
Negatives	Those who experience some loss or damage because of the system implementation, or those who could be adversely impacted by its development (e.g., losing their jobs, losing authority or power for decision making, physical damage, financial losses, etc.).
Responsibles (Execution)	Those who oversee the system throughout all lifecycle phases. This role includes career civil servants and other people inside the public administration, who are working with budgets and schedules (e.g., project manager, public procurement and those responsible for selecting suppliers, etc.).
Decision-makers (Management)	Those who control the process and decide if/how a consensus or agreement must be reached throughout the project.
Regulators and policymakers	Also called legislators or rule-makers. They are generally appointed by government, industry, or civil society to control the quality, security, costs, or other aspects of the system. They generate guidelines that will affect the system development and/or operation. For example, organisations that develop standards, organisations that defend rights, authorities that establish or implement legal and tax controls, etc.
Operators	Those who interact with the system and use its results (information, services, etc.). An operator uses the system but does not necessarily benefit from it. eIDAS node implementers and identity providers can be included in this category.
Advisors and experts	Those who are familiar with the functionalities and consequences of the system implementation. They have deep knowledge about the project domain and can greatly collaborate in requirements elicitation, due to their expertise. Members of DIHs and Advisory Board can be included in this category.
Hired consultants	Any role who provides occasional support to the system development. They are generally external to the organization and are recruited to provide specialized knowledge on a particular area.
Developers (Technical)	Directly involved in the system development (e.g., requirements engineer, analyst, designer, programmer, tester, security engineer, etc.).

On the one hand, this second categorization is more general than the first one, on the other hand it is not, because the first one operates a first very ample distinction between three macro stakeholder categories, that may be extremely useful. Moreover, after the first macro categorization in the first stakeholders classification, the following step is the identification of very specific roles (e.g. identity providers, private trust service provider, etc.) that probably in the present analysis are not so relevant, while the distinction operated in the above table allows to target a more extended group of people while remaining on a general level. It must also be considered that those are the categories that have been adopted within the project. In any case, all the categories of people represented in table 2 fall in fact under the third category of the table 1: the "demand" category. That is due to the fact that the analysis conducted at the beginning of the project was aimed at who represented the final users of the project's outcomes, who could have a decision-making power at the public administration, as well as at the private companies. The current deliverable predominantly addresses the third category, which pertains to demand. This emphasis aligns with the approach adopted in the project. However, the document also includes intermittent explorations into other stakeholders categories. This approach is justified by the emergence of several aspects throughout the project, which, although primarily related to the demand category, may hold relevance or relevance to governance and supply stakeholders.

Having done this preliminary clarification about the project's stakeholders, when a recommendation or a lesson learnt is stated, the present deliverable will also highlight what stakeholder category may be of interest. This approach will allow the reader to immediately locate the parts of the document that may be of interest to him/her and has also the advantage of being more flexible, allowing to underline how a certain recommendation may be in connection with more than one stakeholder category.

4 Definition of disruptive technologies

4.1 Introduction

Till now, the general approach of this deliverable has been defined, together with a delimitation of the stakeholders that will be addressed. **To perfectect the operation of demarcation of the boundaries of the present deliverable, it will also necessary to clearly understand what is the exact meaning – inside the project – of the word "disruptive"**. In other words, when for instance a recommendation about the best way to facilitate the social acceptance of a disruptive technology is stated, how "disruptive" is understood in that particular context will be also delimited and clarified.

This preliminary work is necessary because within the IMPULSE project while of course "disruptive " is used with respect to the technologies that support the IMPULSE eID solution, it is also applied, in a broader sense, to how digital identity management is treated and managed, and to how the framework, in particular the regulatory one, is conceived in a disruptive way and may have such effects.

Therefore, first of all a definition of disruptive technology and of disruptive process will we given, and then, both the disruptiveness of the IMPULSE technologies, and the impact that the process and the framework may have on the society will be examined.

First of all, disruptive technology, firstly conceptualized in Christensen (1997), is defined **as "A specific technology that can fundamentally change not only established technologies but also the rules and business models of a given market, and often business and society overall"** (disruptive technology, 2023). To this regard, it is interesting the excursus that (Hopster, 2021) does on the shift from an extremely negative meaning of the term disruption (i.e. as to break apart from the Latin disrumpere) to a positive one (i.e. as innovation that goes fast and breaks existing, consolidated rules and conventions, that brings radical change).

According to (Christensen C. M., 2013), one relevant characteristic of disruptive technologies is that they introduce products or services that at first are judged to be worse than existing products or that at least are judged with suspicion. However, later on they generate new user needs that previously did not exist and are so capable of reaching a larger market. Also, it is extremely interesting the analysis made by (Schuelke-Leech, 2018) who distinguishes between **first-order and second-order disruptions. The main difference between the two is that while the first is a change localized in a delimited context** (e.g. a market or an industry) **the second one is much broader, affecting entire aspects of** society (e.g. relationships, norms, institutions, policies, or organizations). According to (Schuelke-Leech, 2018), second-order disruptive technologies are complex and dynamic developments of fundamental technologies that are already existing. Often, they combine more than one individual technology and they have ample applications to numerous fields and industries, causing a strong and wide restructuring effect on existing social norms, processes, standards, trends.

This theoretical framework is highly relevant to the IMPULSE project. It is easy to see how the IMPULSE eID solution qualifies as disruptive much more in the sense of second-order disruption than in the first. In other words, the IMPULSE project shouldn't be considered disruptive because it makes use of disruptive technologies such as the blockchain, that from the purely technological point of view are not that disruptive anymore. But it should be considered disruptive because – thanks to the aforementioned technologies – it introduces radical changes in certain social structures, processes, roles, and modifies users' needs and expectations regarding certain fundamental aspects of their being European citizens, as well as the perception of their affordances. Consequently, the approach to the formulation of recommendations and lessons learnt should and will adapt to this framework. Under this approach it is not relevant the industry disruptiveness of a certain technology but rather its social, ethical, legal, and socio-economic impacts.

Another aspect to be considered is the combination of disruptive effects of the proposed solution and of the subsiding regulatory framework, that in some sense combine and mutually empower themselves.

For this reason, a survey will also be here dedicated to the eIDAS regulation and a Proposal to its update (eIDAS 2.0), which lie at the heart of the IMPULSE solution as well as of the EUDI wallet, and to its disruptive effects on the digital identity landscape. It will be useful to understand in full the effects that the introduction of the IMPULSE solution may have and how to successfully cope with them, as well as the need for each country to adapt their laws and regulations and the influence of the regulatory body on the adoption of an eID system like the IMPULSE one (cfr section 6.2.9).

4.2 New Regulatory Framework as Disruptive Transformation

Digital identities are crucial for enabling interactions across diverse platforms and services, serving as the entry point to the digital world. It is imperative to have secure and user-friendly identification solutions to access both public and private services. Acknowledging this, in 2014 the European Union established the eIDAS Regulation (European Parliament and Council, 2014) on electronic identification and trust services for electronic transactions in the internal market (hereafter the eIDAS Regulation or eIDAS). Following a few years of experience with this framework, the European Commission conducted a review, that led in June 2021 to a Proposal to update the Regulation (hereafter the Proposal or eIDAS 2.0). On 8 November 2023, the co-legislators reached a provisional agreement on the text (European Parliament , 2023).

As it will be furtherly clarified below, the introduction of the eIDAS Regulation represented a major change as it had truly transformative effects on the way users, companies and public administrations interact in Europe.

This is the reason why it has been judged relevant to introduce the eIDAS Regulation here, since being something that "lies behind" digital identity systems there is the strong risk of forgetting and underestimating its disruptive effects, that in fact do sum up with the ones pertaining and deriving from digital identity "per-se".

4.2.1 Impact of eIDAS Regulation on the Digital Landscape

The publication of the eIDAS Regulation had a significant impact on advancing the EU digital market. Before its introduction, it was regulated by Directive 1999/93/EC, which had a limited scope, serving as the basis for electronic signatures. Moreover, being a directive, it allowed different transpositions into each national law of EU member states. Instead, the eIDAS Regulation applies directly to all Member States and covers a more extensive range of digital identity aspects, not limited to electronic signatures. In particular, it regulates, electronic identification, website authentication, certificates for electronic signatures, timestamps, electronic seals and electronic registered delivery services.

As a result, **eIDAS has completely transformed how users and companies interact in Europe and also worldwide. Many countries in the world take Europe as a reference for their digital identity standards to establish their legal frameworks concerning electronic activities and transactions.**

4.2.2 The reasons for the eIDAS Regulation updating

Despite the undeniable progress made in implementing the Regulation, the application of eIDAS obtained mixed results. According to the Commission Evaluation, carried out between September 2019 and December 2020, the eIDAS Regulation has only partially fulfilled the objectives set out in 2014. In particular, the Commission Evaluation Report (European Commission, Reports from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), 2014) states, that the eIDAS Regulation has played a crucial role in the further development of the Single Market and in establishing the foundation for the development of the EU identity and trust services market. However, it revealed its limitations to the public sector, including the complexities faced by online private providers in connecting to the system. Additionally, shortcomings were noted in terms of its insufficient availability across all Member States, and its lack of flexibility in supporting variety use cases. There was identified a need for improvements in the Regulation's effectiveness, efficiency, coherence, and relevance to align with new policy objectives, user expectations, and market demands.

The evaluation process also considered that the current market landscape reflects a shift from rigid digital identities to a focus on specific identity attributes related to those identities. This transition underscores that "there is an increased demand for electronic identity solutions that can deliver these capabilities providing efficiency gains and a high level of trust across the EU to services, both in the private and the public sector, relying on the need to identify and authenticate users with a high level of assurance" (European Commission, Reports from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), 2014).

From the findings of the evaluation, it appears that **the eIDAS Regulation was insufficient in addressing the evolving needs of the digital identity market. The limitations of the eIDAS Regulation have prompted efforts to develop a new regulatory framework that aligns with the European Commission's initiative to**

deliver a secure and trusted digital identity for all EU citizens. Specifically, on September 16, 2020, during her State of the Union Address, the President of the European Commission announced the Commission's ambition to deliver a secure and trusted digital identity to all EU citizens:

"We want a set of rules that puts people at the centre. (...) This includes control over our personal data, which we still have far too rarely today. Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used" (European Commission, 2020).

The European Council, in turn, supported the Commission's aspirations and, in its Council Conclusions, called on the Commission to come up with a proposal for a European digital identity framework initiative by mid-2021 (European Council, 2020).

4.2.3 The transformational changes the eIDAS 2.0 would bring

On June 3 2021, the Proposal for updating the eIDAS Regulation was published, accompanied by the Impact Assessment carried out for this initiative. Specifically, the Commission explored various policy options to achieve the Proposal's general objective "to ensure the proper functioning of the internal market, particularly in relation to the provision and use of highly secure and trustworthy electronic identity solutions" (European Commission, 2021). As a result of this exploration, the Proposal largely follows the preferred policy option, which was considered to represent the highest level of ambition and to respond in the most effective and efficient manner to the objectives of the revision.

At present, the long-awaited update of the eIDAS Regulation is progressing towards its formal adoption. The initial text of the Proposal, published in 2021 has changed over these years. After numerous amendments and additions, on November 8, 2023, a Provisional Agreement was reached. Currently, the final text of eIDAS 2.0 is undergoing linguistic revision and translation into all EU languages. Its adoption by the European Parliament plenary and Council of the EU is scheduled in February, and its publication in the Official Journal of the EU is expected in the first quarter of 2024. To ensure proper implementation of eIDAS 2.0, the European Commission will issue implementing and delegated acts. Simultaneously, EU standardisations bodies are developing standards for the new services introduced by eIDAS 2.0. The IMPULSE project in turn, is actively following all processes related to the Proposal to align IMPULSE solution with the eIDAS 2.0.

This **updated Regulation aims to enhance the security and reliability of electronic identification and trust services by establishing a unified European Digital Identity, featuring the European Digital Identity Wallet** (hereafter the EUDI Wallet or EUDIW) **as a key component**. The EUDIW, a mobile application, will be provided by each Member State to their citizens, residents, and businesses to store and manage digital credentials and control their digital identity by deciding who can access their data. Moreover, users will have full control over the data they share with third parties, with the added ability to monitor such sharing. It is not intended to replace existing digital and physical documents; its use is voluntary. Furthermore, it will be free of charge to all natural persons and it will be widely used in both public and private sectors supporting the EU in meeting its 2030 targets for the digitisation of public services (European Commission , 2023) (see figure 2 below).

The EUDI Wallet will provide its owner with access to a variety of services across Europe, including, opening bank accounts, conducting payments, and storing documents such as mobile driver's licenses or professional certifications. This will facilitate faster access to services in travel, healthcare, and various aspects of daily life. Furthermore**, beyond providing convenience, the objective of the EUDI Wallet is to enhance digital trust and security.** Importantly, eIDAS 2.0 mandates Very Large Online Platforms (Google, Facebook, et al) (European Commission, 2023) to accept the EUDI Wallet for login. Moreover, the use of qualified electronic signature will be free of charge to all natural persons for non-professional purposes.

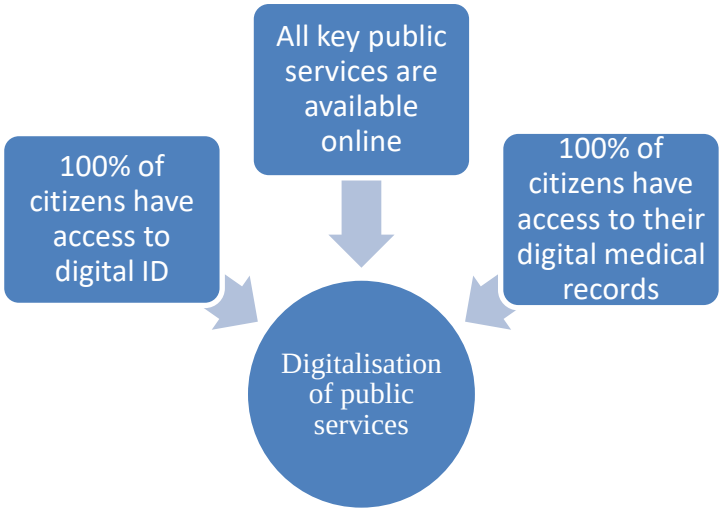


Figure 2 - Digital targets for 2030: Digitalisation of public services

To develop an interoperable solution, ensuring consistency among Member States, and avoiding fragmentation, on 10 February 2023 Commission published the first version of a common EU Toolbox to implement the EUDI Wallet. It includes the core technical Architecture and Reference Framework (a set of common standards and technical specifications as well as guidelines and best practices). Member States keep working with the Commission to continuously update the Toolbox (European Commission, 2023). Furthermore, several multi-year pilot projects are currently assessing the European Digital Identity Wallet and its associated benefits through the Large-Scale Pilots initiative (European Commission, 2023). These pilots, scheduled until late 2024 and possibly extending into 2025, involve more than 250 private and public organisations across almost every Member State, as well as Norway, Iceland, and Ukraine. They aim to assess the EUDI Wallet in real-world scenarios, such as opening bank accounts, applying for university admissions, or requesting a SIM card, highlighting its potential benefits and scalability.

It's crucial to acknowledge that the eIDAS 2.0 will cover more than just the EU Digital Identity Wallet. In particular, eIDAS 2.0 establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, certificate services for website authentication, electronic archiving, electronic attestation of attributes, electronic signature and seal creation devices, and electronic ledgers (European Commission, 2021).

To sum up, **eIDAS 2.0 will have a transformative impact on the European Union, where the EUDI Wallet emerges as a central element, symbolising the future of digital identity.** This updated Regulation provides an opportunity for EU member states which lag behind in advanced frameworks for digital IDs to catch up with the current structures.

However, despite the positive progress resulting from the revision of the eIDAS Regulation, it is crucial to recognise that certain challenges remain. For instance, regarding the impacts on social inclusion and fundamental rights, the previously mentioned Impact Assessment has positive expectations in this regard, but at the same time indicates some obstacles to their achievement. Specifically, while its measures could facilitate access to services for the elderly and people with disabilities, the Impact Assessment also acknowledges the current low level of web accessibility in the public sector. Moreover, it also points out potential barriers, including relatively high user equipment requirements and barriers to technology access, especially for disadvantaged groups.

Furthermore, ensuring consistent implementation of the eIDAS 2.0 across all EU member states is essential, as the initial eIDAS implementation has exhibited variations, resulting in inconsistencies and challenges in utilising electronic identification and trust services.

In summary, the transition from eIDAS to eIDAS 2.0, with the EUDI Wallet as a core element, represents a significant advancement in EU digital identity landscape. IMPULSE solution, aligned with eIDAS 2.0, embodies this disruptive innovation. While recognising its transformative potential, it's crucial to understand and address the challenges related to this type of digital identity system. For this reason, barriers and risks regarding the successful introduction of those systems are explored in the following section.

5 Potential barriers and risks

In section 4 above, the importance of the regulatory framework has been highlighted, also with regard to its potential disruptive impacts. Observed from another angle, the regulatory framework can also constitute a formidable barrier to the successful introduction and implementation of a digital identity system, together with other factors that in the context of the present deliverable must be considered.

In fact, as it was mentioned before, digital identity in its entirety, when introduced into a society, may represent a disruptive transformation and its introduction will consequently not be free of clutches, obstacles and wrong turns.

In the context of a project like IMPULSE, dedicated to the implementation of a system of digital identity management into public services, one of the most interesting outcomes may be represented by the on-field observation (i.e. through the pilots) and by the theoretical reflection regarding the main barriers that can hamper a successful implementation and usage of such a system. These outcomes may represent a valuable result of the project as can be of benefit to any project engaging in similar activities.

For the reasons expressed above, a short analysis will be here dedicated to outlining the possible barriers that act as opposing forces to the implementation and the introduction of a digital identity system. Subsequently, it is addressed the central point of the present deliverable, namely the recommendations and the lessons learned.

The findings here listed are derived from four main sources:

- The feedback received from the pilot's participants (both public administrations and end users) and the outputs of the workshops that have been done in the pilot's countries, with experts and policy makers of that countries.
- The outcomes of the two policy round tables that have been held during the lifespan of the project.
- The survey conducted in the context of the work package 4 on 800 citizens and the analysis of the deriving data made in the deliverable D4.1 v2.
- The main theoretical research being undertaken in the field.

As per the barriers categorization, it has been judged that the approach followed by (Cinar, Trott, & Simms, 2019) may reveal particularly useful in the context of the present deliverable due to its general character and its strict relation to public sector innovation.

For this reason, **the barriers that have been detected and examined during the course of the IMPULSE project will be here categorized into organizational barriers, interaction specific barriers, innovation characteristics related barriers, contextual barriers, barriers related to process stages, interrelations between barriers.** In sections 5.1.1 to 5.1.6 a short explanation is given to each barrier type.

Coming to the single barriers detected, they will be listed all together, accompanied by tags that mark their belonging to one category or to another. This is because each barrier can be placed under more than a category,

At the end of this section, a table will be inserted linking each barrier to the barrier categories and to possible risks deriving from that barrier. Then, the barriers list will be again used in section 6, and it will be connected with the recommendations and the lessons learnt.

5.1.1 Organizational barriers (ORG BARRIERS)

Organizational barriers are barriers that are related to the internal context in which the technology or the innovation is introduced into. Of course, the term must be understood more broadly than its literal sense, because not every context can be reduced to an organizational context. In regard to this type of barrier, besides (Cinar, Trott, & Simms, 2019) and (Cinar, Trott, & Simms, 2021) we follow the approach of (Lukkien, 2023) in which organizational means barriers that are due to various internal factors. Those include "ineffective administration of process activities", "a resistance or lack of support from specific actors", "a resistance or lack of support from specific actors", "a lack of skills, knowledge or expertise" (Cinar, Trott, & Simms, 2021). **Therefore, organizational barriers are related to factors that are entirely dependent on internal characteristics and conditions of the public administration or of the company or of the ecosystem taken into consideration.** In this sense, (Lukkien, 2023) limits his analysis to the internal context. Probably, this is an oversimplification, but it makes the concept more adaptable to the digital wallets use case, that typically insist on a larger context than a simple organizational one. In the context of digital identity systems, the resistance to change and the stickiness to usual practices are clear examples of internal barriers.

5.1.2 Interaction specific barriers (INT BARRIERS)

As the name suggests, interaction barriers **are barriers generated by the interaction between different actors of the process.** They may be due to a lack of mutual trust and/or understanding, to a perception of insufficient benefits from one of the parts, to a scarce governance of the network, or to many other different factors. In the context of a digital identity management system, a typical example could be represented by the public administration that must interact with an external service provider that delivers a set of technical specifications to which the administration must adhere to deliver the digital identity services. As (Cinar, Trott, & Simms, 2021) point out, "within the PSI process, a number of parties are commonly involved, including: public organisations, contractors, citizen groups and NGO`s, political entities, and even international organisations". A hamper may happen at each node of the complex network, and the dynamic nature of this barrier may have the effect of making it extremely difficult to understand and to address effectively.

5.1.3 Innovation characteristics related barriers (INN BARRIERS)

Here the barrier is represented by **the innovation itself, that is perceived as too difficult, expensive, cumbersome, useless, incompatible or incomprehensible by the members of the organization into which it should be introduced.** In the case of public services this may typically mean a public administration, but also a service provider (that has to adhere to new standards or specifications) or even final users, the citizens.

Many of the barriers that will be listed in this deliverable will pertain to this category because it is the one that more has to do with the acceptance of a certain technology and/or innovation in relation to the characteristics of the environment in which it is introduced. For instance, the digital readiness of the country and of its citizens is a typical example of this kind of barrier.

5.1.4 Contextual barriers (CON BARRIERS)

Within the approach that is being here followed (Cinar, Trott, & Simms, 2019), contextual barriers are almost exclusively **barriers related to laws, standards and regulations, to their nature and characteristics** (for instance whether they are too strict or impose too high standards) **and to their eventual absence or incompleteness.** Also, socio-cultural and broader geo-political factors may qualify as contextual barriers, even though – especially in the (Cinar, Trott, & Simms, 2019) analysis – the vast majority of this kind of barriers is represented by laws, regulations and standards.

5.1.5 Barriers related to process stages (PRO BARRIERS)

(Cinar, Trott, & Simms, 2019) operates a **distinction between process stages, and particularly between ideas generation and selection, development and design, implementation and finally sustainment**. This is of course only an instance of many possible subdivision into process stages of a technological innovation project. For instance, since IMPULSE is a research project, only the two central phases have been directly experienced and experimented. In any case, the leading idea here is that the nature and also the effect of each of the aforementioned barriers may change according to the process stage. For instance, a typical case may happen when moving from the design to the implementation phase not sufficient resources are allocated and the project is forced to stop or to scale down because of this. Quite interestingly, in the analysis of (Lukkien, 2023) some of the most frequently emerging (during the workshops and the round tables) IMPULSE project barriers (such as unclear usefulness for citizens/lack of use cases for the IMPULSE digital wallet) are classified under this category.

5.1.6 Barriers list and mitigation actions

5.1.6.1 Lack of practical value for users (including service providers and data issuers)

This issue has been pointed out in almost every occasion in which advice was gathered regarding the main obstacles to the successful introduction of a digital identity system into a country and/or an environment (for example into a municipality or a company**). If users do not perceive the usefulness of the new system, it is extremely difficult that they are going to adopt it, unless forced to by the law or by the context they live in.** This has emerged in particular during both the policy round tables, where experts and policy makers were concordant in identifying this as one of the major issues for a digital identity system adoption. It is interesting on this regard also to check the point of view of (Tsap, Pappel, & Draheim, 2017) that highlights as in the available literature the "functionality" category (meaning "usefulness", "availability of options", etc.) is one of the most recurrent in dedicated papers when considering acceptance factors. The lack of practical value is of course strictly connected (if not a direct consequence) to the lack of (useful) services that can be accessed with the new system. For instance, (Rosca, 2017) examines the case of the introduction of mobile eID in Moldova and finds out that indeed the lack or relevant services is one of the factors pointed out by users as a

reason for not adopting the new identity solution. As we saw in the introduction to section 5 (Lukkien, 2023) moving from the work of (Cinar, Trott, & Simms, 2019) categorizes the possible barriers to digital identity wallets in six possible types (i.e. Organizational barriers, Interaction specific barriers, Innovation characteristics related barriers, Contextual barriers, Barriers related to process stages and Interrelations between barriers) and identify this as related to process stage barriers. This is an interesting approach because this kind of barriers is not related to the eID system itself but to the entire ecosystem and to the relationship between the various actors during the process, bringing to the initial conception to the deployment and introduction of the new system. Quite interestingly, in the same paper are reported the results of a workshop held in the Netherlands, where participants didn't perceive having little functionality inside a wallet as a barrier. On the contrary, they stated that the more you add the more the confusion and the difficulty to use. This to highlight how the point of views, even on something that could be considered universally accepted, are indeed diverse and have multiple aspects. Moving from the outlining of the barriers to the solution, this is of course a problem of communication but also of ensuring the existence of an adequate ecosystem around a new digital identity management system. The last point happens to be also one of the other barriers here listed, because of course if not tackled it represents a problem, while if positively addressed it is part of the solution.

5.1.6.2 Biometrics and data protection

Nowadays, several private and public services are provided online and using eCommerce systems has become very common. It has become possible to access our bank account, book a doctor's appointment or access to state welfare through just a few clicks on a smartphone. Digital identity is the technology at the center of this system, as it enables the shift of the provision of all these services from the real world to the digital world. This digitization of society is a rising trend, however, this also raises some concerns that are needed to address.

Undoubtedly, providing a service over the Internet has several advantages (e.g. scalability, efficiency, speed), but it also increases attack options open to cyber criminals. It is no coincidence that projections by industry researchers and reports by security authorities predict a significant increase in cybercrime in the near future. For instance, Cybersecurity Ventures forecasted that by 2031 the global damage of ransomware alone will amount to US$265 billion. This outlines an outstanding change of pace, as the forecast for 2021 was US$20 billion (Bisson, 2021). Another relevant instance comes from the Internet Crime Complaint Center (IC3), which reported that from 2016 to 2020 the number of cyber-attacks increased by 165% (Hafer, 2021). Given these trends, we can infer that digital threats are not only dangerous, but also here to stay and with wider and cascading impacts.

Therefore, when a public service is provided online it must be protected from the insidious actions of cybercriminals. For this reason, digital identity is protected by a number of measures: these include two-factor authentication, symmetric and asymmetric encryption, and the use of biometric techniques. In particular, the latter has attracted the attention of both private and public institutions, as "the cost of biometric techniques has been decreasing while their reliability has been increasing" (ISO/IEC 24745:2022). The main advantage of biometrics is that they are intrinsically linked to immutable properties of the individual, therefore this can be an ideal technique for the authentication of an eID. This is the approach that has been chosen in the IMPULSE project, as it is based on eID authentication through facial recognition technology. While the comprehensive impact of biometric use is detailed in D4.1, this section focuses on the legal aspects surrounding biometric utilization. These paragraphs are of interest mainly for the citizens/users of the solution, as this analysis on biometrics is based on the GDPR; and for the decision-makers, as a few reflections are pointed to improve the data governance of personal data and exploitation in future projects.

In the realm of eID solutions, biometric data has emerged as a prominent authentication method. Specifically, within the IMPULSE project, a distinct set of biometric data facilitates eID authentication through facial recognition technology. However, this type of technology can pose some challenges. In particular, **the use of biometric authentication techniques creates questions about their compatibility with data protection.**

Therefore, on the one hand, using biometric data (e.g. fingerprint image, voice patterns, iris image and facial image) can be a real asset in creating a trustworthy and secure eID. On the other hand, these very advantages can present issues which must be taken into consideration. But first, let's delve into the legal definition of biometric data, which is provided in Art. 14(15) of the GDPR:

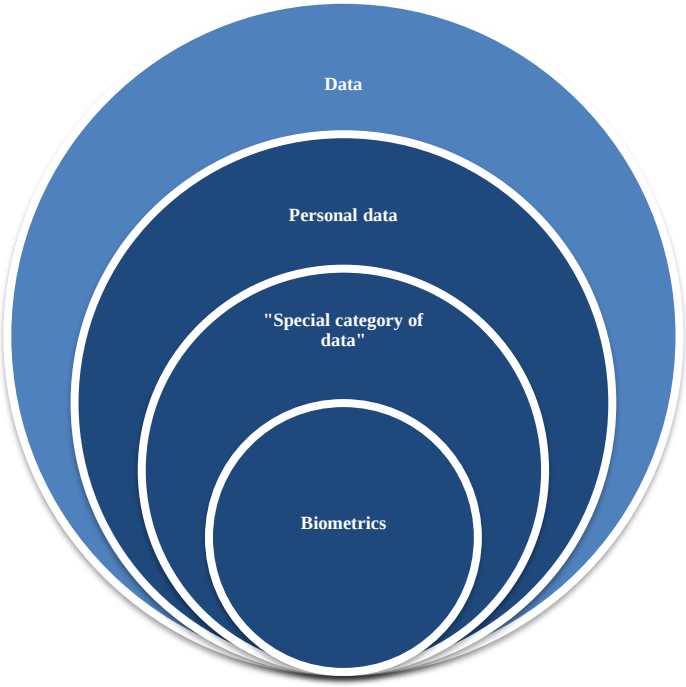
> "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Here, biometric data is presented as a specific sub-class of personal data, which is linked to an individual using physical, physiological or behavioral unique features as identifiers. Interestingly, this kind of data is deemed

in the GDPR as particularly sensitive, as they are listed in Art. 9(1) in a "special category of data" worthy of particular attention. Accordingly:

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, **biometric data for the purpose of uniquely identifying a natural person**, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

To sum up, this means that the use of biometric data not only falls squarely into the regimen of the GDPR, but also warrants particular care. Therefore, it is safe to assume that the processing of biometric data within the European Union is governed by a stringent legal regimen with Art. 9(1) of the GDPR at its core. Accordingly, the latter article enshrines a list of personal data which are deemed as "special" due to their sensitivity, mandating heightened protection and strict adherence to data processing principles. This encompasses the use of "biometric data for the purpose of uniquely identifying a natural person".



The transfer of biometric data outside of the EU/EEA space

The great attention that the GDPR gives to the use of biometric data has brought the IMPULSE project to tackle three legal issues in particular. The first concerns the transfer of personal data outside the EU/EEA territory. According to the GDPR, such transfer is deemed legitimate if supported by additional safeguards and there is a range of possibilities for the satisfaction of this condition. Among them, there is the issuance of an Adequacy Decision (AD) by the European Commission or the establishment of Standard Contractual Clauses (SCCs) between the importer and exporter of personal data (there are other options, such as the exceptions listed in Art. 49 or the binding corporate rules, but for the sake of clarity these paragraphs will not focus on these).

According to Recital 104 of the GDPR, "[the importer] country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union". This outcome can be validated by an AD of the Commission, which essentially recognise the level of data protection in the importer country as adequate. Alternatively, the privacy and data protection of the individuals can be ensured by means of contractual instruments under private law: the SCCs.

Over time, SCCs have become a very popular tool, as they offer an opportunity for standardisation of data transfers between several countries (Determann, 2021). Instead, the reliance on AD is becoming more troubling in certain cases. For instance, the personal data exchange framework between the EU and the US has been brought down by the Court of Justice of the European Union (CJEU) already two times, in the Schrems I and Schrems I cases. Moreover, a third data exchange framework was released in June 2023 - after years of negotiations between the White House and European Commission – but it has already been challenged again before the CJEU.

The security of the transfer of biometric data

A second issue is still related to personal data transfer, but not necessarily to international ones. As aforesaid, the GDPR deems biometric data as particularly sensitive, therefore, also the security of the data processing must be ensured with particular care. This encompasses the protection of biometric data not only when stored, but also when transmitted; especially when the recipient is located abroad. Man-in-the-middle attacks and the improper handling of personal data by the recipient are scenarios that must be taken into account when these security measures are designed. Some considerations can be noted on this point, based on the experience gained within the IMPULSE project.

Ascertaining the Level of Assurance as a security and business enabling measure

The third point is still related to security of data processing, but from the perspective of authentication that behind an eID there is the rightful owner. Indeed, as stated in the ISO/IEC 29115:2013l, "the confidence placed in all the processes, management activities and technologies used to establish and manage the identity of an entity for use in an authentication transaction" is a very important part of security inside the digital world. The degree of this confidence can be classified in different ways depending on the reference framework, for example in ISO/IEC 29115:2013 it is broken down into 4 distinct Levels of Assurance (LoA). Differently, within Art. 8 of eIDAS are listed 3 LoAs: Low, Substantial and High. Accordingly

- The LoA Low express a limited level of confidence and is compatible with single-factor authentication (e.g. only a password/username). Moreover, it corresponds to the LoA 2 inside the ISO/IEC 29115:2013.
- The LoA Substantial provides a solid guarantee of the claimed identity, as such, this level is useful for eID authentication. This level is compatible with the use of a two-factor computer authentication system and it corresponds to LoA3 of the ISO/IEC 29115:2013.
- The LoA High provides the highest degree of confidence in the claimed or asserted identity of a person through eID. This level is compatible with the use of two-factor authentication, digital certificates and private key. It corresponds to Level of Assurance LoA4 of the ISO/IEC 29115:2013.

It must be highlighted that the level "Substantial" and "High" are privileged by the eIDAS Regulations, especially for accessing the services of the PAs. But at the same time it is important to keep in mind the tradeoff between security and usability of a solution. Therefore, reaching the LoA "High" might not be advisable in every use case. The IMPULSE Consortium conducted tests to assess the LoA of the IMPULSE Solution, as documented in D5.2. At the end of these trials it was reported that according to eIDAS classification, IMPULSE achieves LoA "Substantial". Although this can be categorized as a very good result, further testing would be advisable in the future: defining the LoA is very important, as it is on the basis of it that in practice the solution will be able to perform certain type of actions and the complexity of the security measures.

5.1.6.3 Concerns about a unique persistent identifier

The unique identifier represents a part of the minimum data set of person identification data, which is available from electronic identification schemes, and is already required by the eIDAS Regulation. This set, in particular, includes current family name(s), current first name(s), date of birth and a unique identifier "constructed by the sending Member State […] for the purposes of cross-border identification and which is as persistent as possible in time" (European Commission, 2015).

Nevertheless, it appears that this set has proven insufficient. Following the Impact Assessment Report of the Proposal, over 70% of Member States reported that "the rigid data set for notified eIDs makes it also difficult to match identity records as the current minimum dataset is often not sufficient to uniquely identify a person" (European Commission, 2014).

Therefore, the initial version of the Proposal stated that the interoperability framework for electronic identification had to include a reference to a minimum set of person identification data to uniquely and persistently represent a natural or legal person.

This created the possibility to link different information about a person together, something that becomes beneficial because has as an effect that individuals are spared from repeatedly providing the same information or requesting it from one public service to share with another. The services can exchange the required information, and it remains feasible to identify a person and link her to database information even in cases where there are changes in her name or address.

However, there is a dark side to this possibility. First of all**, representing a person uniquely and persistently could be problematic from a privacy-by-design point of view.** A persistent identifier poses the risk of linkability, allowing all information about a person to be connected and a complete profile to be made, without

individuals knowing that this is being done, potentially disadvantaging them. The fact this unique identifier is persistent means that it can connect all information throughout a person's life, even in cases of name changes or relocations, and no desire to link it to old information anymore. Its consistent use across sectors and contexts can facilitate unlawful data exchange, aggregation and profiling.

Moreover, **an eID system based on persistent identifier, can pose serious problems of privacy and traceability because of power imbalance issues**. The user may be forced or tempted to give away his personal data in exchange for a service he wants or needs or simply to speed up access (Martin, 2023).

Furthermore, the mandatory inclusion of a persistent unique identifier invalidates any practical use of pseudonyms under eIDAS Regulation Article 5, as any pseudonym could be associated with identifying information and become a de facto unique identifier.

Additionally, some Member States have used the discretion granted by the Art. 87 of GDPR, which states that "Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application", by specifically prohibiting the use of unique identifiers (e.g. Germany) or not prohibiting but it is strictly regulating (e.g. Austria).

Is important to notice that in the Provisional agreement on the Proposal, reached on 8 November between the European Parliament and the Council, which could be considered the latest version of the Proposal, there is no more the requirement for a persistent, unique identifier as a requirement for the minimum set of personal identification data because it has been recognized that the risk of misuse outweighs the advantages. However, it does not contain an explicit prohibition regarding unique persistent identifiers, something that leaves the door open for further developments on this topic and may raise serious concerns, representing a formidable barrier to a successful introduction of an eID solution.

5.1.6.4 Lack of transparency, security not sufficiently ensured

Trust is for sure one of the main factors sustaining the positive introduction of a digital identity system. **While a positive attitude towards digital identity can only be built on trust, trust inturn relies on two main factors: transparency** (nothing is voluntarily hidden, the citizen can freely and easily access to all the relevant information) **and security**. Where these two are ensured, it's not immediate that trust follows, but it's certainly easier. Transparency, as security, must be actively sought, designing the system and the product from the beginning in such a way that these vital factors are ensured. This was strongly pointed out during the French and Danish workshops, where the question of trust emerged as one of the key issues, while in Italian and German workshops the questions of privacy and cybersecurity were identified as central for a successful introduction and adoption of a new eID system (to access an expanded report about the outcomes of the workshops, please refer to the D6.2 deliverable, where there is a synthesis of each workshop as well as the actual questions and answers).

Clearly, this is not a completely new finding, since it is possible to find multiple similar case studies in this respect. For instance, (Alkalifah & D'Ambra, 2013) examine how initial trust perceptions influence the user intentions to adopt an identity management system, while (Khan & Abideen, 2023) indicate perceived trust as having a "strong moderating effects on the relationship between perceived risk and digital wallet usage behaviour". (Halperin & Backhouse, 2012) highlight as a **lack of trust may be due to beliefs in public authorities** responsible for identity management, influenced on its turn by the dimensions of competence, integrity and benevolence, usually built on negative past experiences.

As a consequence of the general convergence on this aspect, it may be interesting to understand and highlight which factors do affect trust in a certain digital identity management system, so as to overcome the possible barrier represented by a lack of trust.

5.1.6.5 already existing digital identity systems, interoperability, standards

Why burden oneself with the learning and the difficulties connected with the introduction of a new digital identity system where there is another one already in force and perfectly working? This point was particularly stressed out during the Italian and the Nordic countries workshops, as well as in the Danish one: in all these countries there are already working and widely used public eID systems, so the problem of market saturation indeed exists. Nevertheless, during the first and the second policy round table this aspect was mentioned by more than one of the participants (cfr the D3.5 and D3.6 deliverables). It could be the case because the new system allows processes that with the previous system were impossible, because it enhances security, or privacy, or usability, or because it grants access to more services. Moreover, this is connected to many of the points listed here (e.g. lack of practical value, access to a wide range of services, insufficient ecosystem, and usability. In addition, interoperability might be an important asset to overcome. **If the new system is**

interoperable with the existing ones, the citizen might have more time to experiment with both and better perceive the advantages of moving to the new one. Probably, this will be the approach that the European Commission will adopt for the introduction of its digital identity wallet (i.e the wallet as co-existing with traditional national eID systems). This is particularly evident in the outcomes of the Italian and of the Nordic countries (Iceland, Finland) workshops: in both it was pointed out how the presence of already working national eID systems would represent a strong barrier to the introduction of a new system and that it would have been necessary a great communication effort to make understandable to citizens the necessity and opportunity of introducing a further one (cfr deliverable D6.2).

5.1.6.6 insufficient ecosystem, including awareness, digital divide, presence of adequate infrastructures, availability and kind of devices

The introduction of a new digital identity system does not happen in a neutral environment. On the contrary, it typically happen in societies that present many complexities and stratifications, and it is needed exactly for this reason. In this view, **the entire ecosystem in which the new system is introduced must be considered and can represent a formidable barrier, including the regulations and laws in force, the infrastructure, the awareness and the level of technological savviness of the population, the service providers and the verifiers, the maturity and number of services available**. This was particularly evident from the results of the Peshtera pilot, where the original IMPULSE implementation plan had to be scaled down due to contextual technical and legal limitation. In particular, in the background report of the D6.2 deliverable it is reported how e-governement services have been introduced in Bulgaria before a solid eID infrastructure existed and this generated a scarce penetration and usage of the available systems by the population, combined with a diffused lack of trust because of prior data leakage issues.

In the context of the IMPULSE project a PEST analysis examining the external factors that may influence the project's outcomes (cfr. deliverable D7.3) was conducted, and infrastructural factors obviously emerged as one of the key points possibly impacting the project. In particular, the investments in digitization and the availability of high-speed internet into a country, as well as the availability of devices, were highlighted as a major impact factor. Quite interestingly, during the second policy round table multiple policy makers pointed out the importance of attentively considering also the verifiers and their interests, without forgetting that the system is for the entire ecosystem and not only for the citizens (cfr D3.6).

Privacy issues should be taken into account as part of the global awareness question. However, during the review conducted in the context of the WP4 it emerged that the majority of users would be ready to give out some bits of privacy and data protection if they had access to truly valuable services (cfr D4.1 v2). In the light of these results, we could consider service availability and infrastructural aspects as the leading elements of the digital identity ecosystem and of the connected barrier.

5.1.6.7 existing (and perhaps different) regulations, country structural solidity

In the EU there is a strong and focused attention to the regulatory aspects of identity and personal data management. With the GDPR and eIDAS and eIDAS2 regulations the EU is trying to establish a common regulatory framework that also allows cross border identity management for EU citizens, as well as equal rights and capabilities. However, beyond the aforementioned general frameworks, at local level different regulations and interpretations may govern all the details and aspects of digital identity management, and if not adequately addressed they may represent a huge obstacle to the positive and correct development of a working digital identity system.

This factor was represented as a barrier in the course of the Bulgarian workshop and during the second policy round table, and it has been also widely represented in the literature. For example, (Cinar, Simms, Trott, & Demircioglu, 2022) classifies regulatory barriers among the contextual ones, and illustrates how current laws, policies and regulations may represent one of the dominant contextual barrier that innovators had to face during their attempts to introduce a new service or technology.

Another aspect that should not be underestimated pertains to the structural solidity of the country in which the digital identity system is poised for introduction. Research in this field indicates that **citizens are more inclined to place trust in a digital identity system if the proposal originates from a nation with robust political and economic foundations**. The rationale behind this is quite evident, as individuals are more likely to trust actions and proposals emanating from a source that has demonstrated adept management capabilities. This facet has consistently surfaced during workshops and roundtable discussions conducted throughout the project's duration.

This point is discussed also in (Friedhoff, Cam-Duc, Ladnar, Stein, & Zureck, 2023) where it is stated that citizens' personal trust in the government and in providers/companies also plays an important role. According to this research, citizens tend to disclose their data more in "secure and structurally strong" countries, which also increases the willingness to use wallet apps to manage their data."

5.1.6.8 Usability

If a solution is overly complicated, places an excessive cognitive burden on the user, requires a learning steep too high, it is highly probable that it will not be easily adopted. During both the first and the second policy round tables this aspect was stressed out by many of the participants. Of course, there is a vast literature about the connection between usability and acceptance of technology. In particular, in (Khan & Abideen, 2023) usability is correlated directly with intention to use e-wallets and many other contributions on the same topic are reported. While the other barriers are mostly external, this one pertains entirely to the design of the solution and to its frontend. Users should be engaged since the beginning, and usability experts should be consulted and enrolled to ensure that using the new solution is not burdensome, or that it is not more burdensome than other existing solutions, including traditional physical id cards.

Usability affects users on multiple dimensions. Firstly, users' willingness to adopt the solution can be altered by over complicated features. Secondly, any feature that is not strictly necessary may be an unintentional form of exclusion, since the more complex the system is the more non digital native people could refuse to use it. Moreover, usability is important to reduce the number of errors by users. Because of Digital Identity solutions' role, errors can have tremendous consequences, therefore it is of paramount importance to avoid conditions that lead users to confusion and errors. Finally, usability is strictly connected to trust. Users feel safe when they can understand simply how to use a system. A usable system is often considered by users as trustable because they can understand the reason behind every step that they have to do to use it correctly. An excessive number of steps may be perceived as a reason to not trust the solution.

Table 3 - Barriers' categorization

BARRIERS	Organizational	Interactional	Innovation	Contextual	Process
5.1.6.1 Lack of practical value for users (including service providers and data issuers)				✓	✓
5.1.6.2 Biometrics and data protection		✓		✓	
5.1.6.3 Concerns about a unique persistent identifier	✓		✓		
5.1.6.4 lack of transparency, security not sufficiently ensured			✓		✓
5.1.6.5 already existing digital identity systems, interoperability, standards			✓	✓	
5.1.6.6 insufficient ecosystem, including awareness, digital divide, presence of adequate infrastructures, availability and kind of devices	✓			✓	
5.1.6.7 existing (and perhaps different) regulations, country structural solidity		✓		✓	
5.1.6.8 Usability	✓		✓		✓

6 Recommendations and lessons learnt

After clarifying in the context of the IMPULSE project and of its developed theoretical framework the meaning of disruptive technologies and innovations, identifying the target stakeholders and outlining the main barriers faced by eID projects in general and the IMPULSE project in particular, the present section will highlights the lessons learned by the consortium on how effectively advancing such a complex project. Additionally, it aims to provide some hints and suggestions for the future endeavors.

The areas we concentrate on are the ethical and legal aspects of the introduction of an eID system, the socio-economic issues, and the standards, that are an important albeit sometimes underestimated point.

For each area the main points emerging from the work done during the IMPULSE project lifespan are discussed, and some possible critical points and recommendations are introduced. At the end of each subsection a table is included with the indication of which stakeholders and/or barriers refer to each recommendation.

6.1 Ethics and Legal

In line with the European Commission dictate, the IMPULSE solution is based on an SSI approach, with the final aim of empowering citizens regarding the use of their personal data and of the related consents.

As highlighted in the deliverable D3.3, SSI brings forth a paradigm shift in how we perceive and manage digital identities. As we navigate this transformative landscape, it is imperative to embed ethical considerations into the very design of SSI systems.

eID solutions based on an SSI approach share – as highlighted in deliverable D3.3 – a set of values and principles that lie at the basis of each implementation, including the IMPULSE one. In the table 4 below (taken from deliverable D3.3) the main values and principles are listed.

Table 4 - SSI approach values

Value	Description	Principle
Wholeness	The user is not separated by his data	Existence, Persistence, Protection
Autonomy	The user must be central to the administration of identity	Control, Access, Minimalisation, Consent
Shareability	The user must be able to decide to share an identity from one service to another	Transparency, Portability, Interoperability

In the case of SSI approaches to eID individuals have full ownership of their data, where this ownership is an inherent right. The power to control their data stems from an innate right to self-governance, independent of external authorization from other individuals or institutions. This right is established based on natural characteristics that inherently grant citizens their digital identity. These citizens, being the sole bearers of these unique attributes, are the only ones identified by them, underlining their singularity and distinctiveness. In terms of identity management, sovereignty is defined as the capacity to distribute validated credentials with a preference for revealing the least amount of personal data possible, allowing individuals to exert authority over their sensitive identity-related information.

As already underlined in D3.3, there is a subterraneous conflict in Identity Management solution between approaches that prioritizes individual rights and other that considers societal needs, dependent on the on the value system intrinsic to a specific society at a given historical juncture (Ishmaev & Stokkink, 2020). Individualistic values such as self-determination, moral autonomy, and rights to privacy and data control can ideed be in contrast with communal values like accountability, societal obligations, and responsibility for one's actions (Ishmaev, 2021). In designing an Identity Management System, there is an inevitable decision-making process that involves favoring certain values over others (Pierucci & Cesaroni, 2023).

The SSI model emphasizes individuals' sole ownership and control over their own credentials. In this model, there exists a unified online persona, promoting individual autonomy while necessitating user awareness (Zwitter & Gstrein, 2021). This model is fundamentally built on principles such as ownership of data, autonomy in managing one's identity, acknowledgment of inherent attributes, distinctiveness, and individuality. These concepts are encapsulated in the SSI's ten guiding principles: existence, control, access, transparency, persistence, portability, interoperability, consent, data minimization, and security and lie at the basis of the ethical assessment that has been done in the context of the IMPULSE project (see D3.3) as well as of the recommendations that will be listed and discussed in this section.

In this section these aspects as well as the emerging ethical and legal critical points are highlighted, with a particular regard given to the issues deriving from the use of biometrics. In fact, as a cornerstone of identity verification, biometrics raises intricate questions about consent, security, and potential biases. The section dedicated to this matter will delve into the ethical implications of biometric data usage, shedding light on the critical points that warrant consideration from both an ethical and legal perspective. SSI introduces important ethical and legal considerations that demand meticulous examination as it isn't a one-size-fits-all solution: it has limitations and potential drawbacks. European-wide adoption of SSI may not fully address historical issues with digital identity and may even expose individuals to vulnerabilities (Giannopoulou, 2023). Critical evaluation of the underlying ideologies and assumptions of SSI is necessary to ensure its responsible and effective implementation. Therefore, best practices in data governance are suggested thanks to the experience from the project unified with literature insights. In the end, the actual impacts of an SSI approach are discussed and possible recommendations on this regard are suggested, as well as the importance of regulatory aspects for the successful introduction of an eID system.

As a first result, from the work done and the evidences gathered so far it strongly emerges the importance of embedding ethics in all the phases of a digital identity system design and development (Marsman, 2022), adopting a veritable ethics by design approach, and ensuring that ethical principles guide the development and deployment of SSI solutions. The next section indeed delves into these aspects.

6.1.1 Implications of an ethics by design approach

In the realm of SSI, trust is paramount, and it is earned through transparency, accountability, and a profound respect for user autonomy. By embedding ethical principles into the core of SSI development, not only potential risks and pitfalls are mitigated but also the evolving concerns of the digital society are proactively addressed. In doing so, SSI systems are elevated from mere technological solutions to ethical frameworks that respect the dignity and agency of individuals.

Moreover, an Ethics by Design approach acknowledges the dynamic nature of technology and the ethical challenges it presents. It calls for continuous evaluation, adaptation, and improvement, ensuring that ethical considerations remain at the forefront of the rapidly evolving SSI landscape. This approach recognizes that ethical responsibilities extend beyond the initial design phase, encompassing the entire lifecycle of SSI systems.

In essence, **an Ethics by Design approach is a commitment to building more than just secure and efficient digital identity solutions.** It is an effort to construct systems that reflect collective values of a certain society and culture, where users are not mere subjects but active participants in shaping and controlling their digital identities. This proactive stance toward ethics is not only a safeguard against potential misuse but also a proactive step toward fostering a digital environment that promotes inclusivity, fairness, and the broader societal good.

Following, some of the main issues and related mitigation actions and recommendations that came to light regarding this point are examined.

6.1.1.1 Technology systems and in particular eID systems are value laden, a careful approach should be undertaken to be sure that the (ethical) reached outcomes correspond to the desired ones

It is necessary to explicitly incorporate an ethical reflection since the beginning and an ethical monitoring during all the phases of the project to be sure to incorporate and then convey the desired values in the eID solution that is being developed and delivered. While it is unavoidable to transmit values (e.g. the point about the sovereignty of the individual on his identity and his data, that is obviously conveyed through an SSI model) it is necessary to explicitly include public values in the design of eID solutions and so to have clear before starting what these values are. As it was pointed out by one of the participants to the second policy round table

(cfr D3.6) **the technology also impacts on perceptions, and it is possible to translate it into a higher level of rights and obligations.**

6.1.1.2 The new European eID approach has a great "educational" potential hidden inside, to make European citizens more aware of their rights regarding personal data protection. Take advantage of it to take a step further in the construction of a more equitable society

In section 6.1 it was highlighted how any technological system is value laden, and how it is necessary to make hidden values explicit. Another step in this direction is deciding to explicitly convey certain values so that the adoption and usage of a certain eID solution also have the effect of changing the users for the better, for example making them accustomed to personal rights protection or to the necessity of protection of certain social groups (for instance minors) from the effects of online interactions. This educational potential should be attentively studied and addressed in a dedicated way.

6.1.1.3 When designing technological systems, inclusiveness is often underestimated in the design phase, obtaining results that are not fully inclusive. Actions should be undertaken to avoid this pitfall

Design teams should include from the beginning representatives of people with disabilities and/or of people at risk of social and digital exclusion. The approach should not be that coping with disabilities or with other reasons of exclusion forces the design to eliminate things or to lessen the complexity. On the contrary, it should be common understanding that the world that has to be reflected and incorporated into the design of an application or of a product is more complex and rich than is usually considered to be and that this must be incorporated and reflected into the design and the development of a product. This means more instead of less functionalities. The **design should rather start from the inclusion, having it at its core, and then move further on, to cover all the other aspects.** Only in this way a product can be certain to be fully inclusive and to not leave behind anyone. In other words, as one of the experts participating in the IMPULSE policy round tables and Expert Advisory Board stated, edge cases must be treated as central, because from that approach do derive an approach capable of being truly humanistic, in the classical meaning of the term.

6.1.1.4 The introduction of an eID solution like IMPULSE if not done correctly has the potential of broadening the already existing digital divide and to create new areas of exclusion. An attentive analysis must be done during the design phase, taking into account also the different societal contexts, to avoid this negative consequence

The significance of a project such as IMPULSE is underscored by the fact that its pilot initiatives are being implemented in a wide array of socially and nationally diverse contexts. This emphasis aligns with a viewpoint prevalent in the scientific literature devoted to innovation management, highlighting the imperative to meticulously analyze each distinct context. It is essential to **comprehend beforehand whether the introduction of a new eID solution could potentially yield undesirable consequences.** Undoubtedly, there is a risk that a segment of the population, particularly social groups susceptible to digital exclusion (refer to D4.2), may be inadvertently marginalized or left behind.

6.1.1.5 Adopt a citizen-centric approach, that implies taking since the design phase all the necessary actions to protect the citizens, not leaving on them the burden of protecting themselves. This implies implementing a regulatory control to avoid the power imbalance between the citizen and the service provider and prohibiting to ask for data that should not be asked

During the second policy roundtable, a crucial point was highlighted: during the design phase, the pertinent question should be "where can I abuse?" instead of "how can I use?" The objective is to envision, and **preemptively prevent through design, all possible avenues where the system might be exploited to the detriment of citizens, institutions, issuers, or verifiers.** The burden of safeguarding oneself, such as avoiding consent for unnecessary personal data usage, should not fall upon the user. Rather, the focus should be on prohibiting the unnecessary collection of personal data. In essence, this issue is, or should be, a matter of policy rather than relying solely on the design of the technological solution.

6.1.1.6 Do not make identity system dependent, to avoid creating exclusion areas and/or issues in case of unavailability of service or of system failure

This, together with the strictly connected aspect of the interoperability between different eID systems, is a theme that received much focus during the second policy round table but also in occasion of the country workshops (D.6.2). The fact that **digital identity should not become the ONLY method of identification** has been advocated by many experts and stakeholders during project workshops. Not only because of the

possibility of a system failure, but also because digital identity can more easily generate exclusion areas. Better to think of digital identity as another mean of identification that will be freely used alongside other traditional methods of identification, that can continue to be used.

6.1.1.7 Meditate attentively whether it is truly necessary to authenticate

Identification and authentication even if they are made easy and immediate are nonetheless an action that requires a certain amount of effort on the user part and can even create exclusion areas. For this reason, parallelly to designing an eID solution that is truly usable and accessible a reflection should be dedicated to what the limits of identification should be, and define the cases where it is absolutely necessary, where it is desirable and where it is in fact useless to formally identify and authenticate a person**. Many services and contents could be accessed without need of identification** and pursuant to the principle of minimization of the requested data should not ask the user to authenticate

6.1.2 Biometrics

Biometrics, while offering a robust means of identity verification, poses multifaceted ethical challenges. The very nature of biometric data, often unique and sensitive, requires a delicate balance between security imperatives and the preservation of individual privacy. Striking this balance is not only a technical challenge but also an ethical one. The ethical dimension of biometrics in SSI systems underscores the need for transparent and user-centric practices. Users must be well-informed about how their biometric data will be utilized, stored, and protected. Informed consent becomes a linchpin, necessitating clear communication about the purposes and potential risks associated with biometric data processing.

Implementing robust ethical guidelines for biometric data collection, storage, and usage is imperative. Such guidelines should address issues of consent, ensuring that individuals have the agency to control how their biometric information is employed. Additionally, ethical considerations extend to the potential biases embedded in biometric algorithms, emphasizing the need for fairness and non-discrimination.

6.1.2.1 Legal aspects regarding the transfer of biometric data abroad

As previously mentioned, the GDPR establishes a framework for the transfer of personal data. In particular, there are specific aspects that must be taken into consideration when personal data are sent outside the EU/EEA space. These **transfers need to be supported by additional requirements**: they can be (not exhaustively) an AD from the European Commission, or the signing of SCCs by the Exporter and Recipient of the personal data.

However, 5 years after the implementation of the GDPR, practice has shown some critical issues in the use of Ads, in relation to their instability. Specifically, the work of the EU Court of Justice has over time highlighted and clarified some of the data protection parameters that foreign jurisdictions must meet in order to be deemed "equivalent" to European jurisdictions. This work of clarification has, however, had the setback of caducating two very important ADs with a trading partner such as the United States.

The current view is that the situation will not stabilize in the immediate future, so it is proper to arm oneself with alternatives to AD wherever possible, such as drafting SCCs. This is even more important in the case of IMPULSE, as this project deals with biometric data: a category of personal data regarded with particular apprehension within the GDPR and, therefore, particularly protected.

6.1.2.2 Legal aspects regarding security of biometric data

As stated earlier, the transfer of biometric data requires special attention to confidentiality, security and, more generally, data protection. Along these lines, the experience within the IMPULSE project has shown that this can only be achieved collectively by the consortium and not by individual partners. There are standards - such as the celebrated ISO/IEC 27001:2022 - that are calibrated to certify the security of the data flow within a company. But within a consortium such frameworks may not be sufficient because (apparently) they take into account only individual entities and not the consortium as a whole. For instance, if personal data are sent abroad (e.g. for the use of a cloud provider), they should be encrypted in a proper manner and every member of the consortium must be aware of this aspect when they select an external provider.

For this reason, it is recommended that **for better protection of personal data (especially if it is biometric data) the concert of security measures as a consortium.** All partners need to be aligned and aware of these measures. These may also include important technical measures for the transfer of personal data such as the proper use of cryptography. Here, a framework such as the ISO/IEC 27001:2022 might be useful and provide

guidance on how to ensure confidentiality, integrity and availability within the whole consortium. This can give a boost to the data processing security within the consortium:

6.1.2.3 Legal aspects of biometric authentication

Among the measures that can be used to ensure the security of a digital system there is authentication, which in the IMPULSE solution employs biometric data. However**, authentication has implications that go beyond security and data protection.** Specifically, according to eIDAS, the specific qualities of an authentication system can have profound repercussions on the practical possibilities of a eID solution within a real-world scenario. In eIDAS the LoA of a eID can be "Low", "Substantial" and "High": depending on the level of LoA that the chosen eID solution reaches, different use cases qualify. During the development of these solutions, all the partners (especially decision makers) should be aware of these aspects, because it is also from these that it will be possible to understand the actual potential of a solution.

6.1.2.4 How to cope with mistrust regarding biometrics

From theoretical (c.f.r D3.3) as well as on field (c.f.r D4.2 and D6.2) analyses it results that when considering biometrics identifications the point that people are more scared about is violation of privacy (with connected data storage and secondary use) and pervasive control. A great effort should be made to **correctly communicate the way in which these aspects are taken into account and solved inside eID solutions and how risks are mitigated.** Human in the look mechanisms for onboarding should be maintained even though fully automated onboarding could be possible.

6.1.2.5 The importance of previous experiences with biometric identification

From the analysis conducted in the context of the work package 4 and whose results can be found in the deliverable D4.1 it results that, especially in certain countries such as Germany in which the concern about privacy are higher, biometrics may be a big source of mistrust. However, having had a previous positive experience with this technology greatly mitigates the possible distrust. This can be generalized to all kinds of technology. A possible recommendation to derive from this finding may be to **make available smaller and simpler services and/or tools that make use of the technology before the introduction of a major tool or service that is based on that technology**, to allow people to become accustomed to it. The same result can be obtained through communication or educational campaigns.

6.1.3 The importance of increasing awareness and trust

Increasing awareness and trust in SSI systems is pivotal for their successful adoption and societal integration. This section explores strategies to enhance awareness and trust, recognizing the importance of transparent communication, educational initiatives, and user-centric design. Moreover, trust frameworks and interoperability are foundational for the success of SSI ecosystems, especially in cross-border and cross-organizational scenarios.

6.1.3.1 How to promote awareness and its importance for a successful adoption

Inside the IMPULSE project a co-design and co-creation methodology has been adopted as well as a policy of continuous contact with digital innovation hubs and with field experts. These are actions that have good potential to deliver good results with respect to the objective of increasing awareness and of conveying the project's approach and results, furthermore with a single country focus, as they are pursued in each single country. In general, this is an approach that can also be generalized: exploit the design and the development phases of an eID solution to foster awareness in the main stakeholders and to generate interest and a positive approach.

Within the dynamic landscape of the IMPULSE project, the adoption of a co-design and co-creation methodology underscores a proactive approach to promoting awareness and fostering the successful adoption of SSI systems. This methodology involves continuous collaboration with digital innovation hubs and engagement with field experts, forming a robust framework for knowledge exchange and refinement of SSI concepts.

The utilization of co-design and co-creation methodologies acts as a catalyst for inclusivity and diversity in the development process. By involving stakeholders from various backgrounds, including end-users, developers, and policymakers, the project ensures that the awareness-building strategies are tailored to address the specific needs and concerns of diverse audiences. This approach not only enhances the quality of the awareness initiatives but also lays the groundwork for a more universally accepted and understood SSI ecosystem. Continuous contact with digital innovation hubs serves as a strategic avenue for staying abreast of

the latest advancements in technology and understanding the evolving needs of the digital landscape. These hubs, often at the forefront of technological innovation, provide valuable insights into emerging trends and potential challenges, enabling the IMPULSE project to adapt its awareness-building strategies to align with the current state of the art.

Field experts, with their deep domain knowledge, play a pivotal role in refining the messaging and educational content related to SSI systems. Their contributions ensure that the awareness-building initiatives are not only accurate from a technical perspective but also resonate with the broader societal implications of adopting SSI. By involving experts in the process, the IMPULSE project gains credibility and ensures that the information disseminated is reliable and trustworthy. The project's commitment to a single-country focus further emphasizes the importance of tailoring awareness strategies to specific contexts. **Recognizing that cultural, legal, and social factors can influence the reception of SSI, the project adopts an approach that resonates with the unique characteristics of each country**. This nuanced strategy acknowledges that a one-size-fits-all approach to awareness building may not be effective, and customization is essential for ensuring the relevance and impact of the initiatives.

6.1.3.2 Trust as the key to successful introduction on an eID solution: how to nurture it

Trust in eID solutions has been indicated (D3.6, D3.5, D6.2 v2) as strictly intertwined with transparency, but also with the general attitude towards the country considered globally: its political stability, its approach towards citizens' rights, etc. So, for sure it's essential to communicate constantly with stakeholders (not only citizens but also service providers, issuers, etc), coping with possible issues and not hiding pitfalls or dead ends, but also to adopt an holistic approach, taking into account the entire approach of a country. For example, in the D4.1 v2 deliverable it is clearly highlighted how the approach to welfare of a country directly influences the grade of digital inclusion and the propensity to adopt. Therefore, the recommendation here is to avoid focusing only on the specific matter of digital identity and the strictly related topics but to maintain instead an ampler look at the context, to avoid that un-considered elements have an unexpected influence on the outcomes. Transparency emerges as a cornerstone in the establishment and maintenance of trust. Users need to have a clear understanding of how the eID solution operates, how their data is handled, and the overall security measures in place. It is essential to communicate openly about the processes, potential challenges, and even limitations of the eID system. This transparency not only instills confidence in users but also fosters a sense of accountability among service providers and issuers. **The recognition that trust extends beyond technical considerations to include the overall stability and governance of a country is a key insight**. Political stability and a commitment to citizens' rights are integral factors influencing the overall perception and acceptance of eID solutions. Therefore, maintaining an ongoing dialogue with stakeholders on these broader aspects is essential for building a solid foundation of trust.

A holistic approach is recommended, urging project stakeholders not to narrow their focus solely on the specific technicalities of digital identity. Instead, they should broaden their perspective to encompass the socio-political landscape. By considering these broader implications, the project aims to prevent unforeseen elements from impacting the outcomes and to align eID solutions with the broader goals of societal progress.

The recommendations put forth in this section emphasize the importance of open and honest communication with stakeholders. This includes addressing potential issues head-on and avoiding the concealment of challenges. In doing so, the project seeks to foster a culture of trust that goes beyond the immediate context of digital identity, permeating the broader perceptions of the technological landscape and its impact on society.

6.1.3.3 SSI and decentralization are not per se keys to increasing trust

If the users trust the centralized authority that issues and stores data, they could have a better attitude towards it than with regard of a technology and of a concept that they barely understand. It isn't sufficient to speak of SSI to gain the trust of potential users, the gains and the advantages must be thoroughly explained before they can be of any utility for the cause of adoption. The assertion that users inherently trust decentralized systems is nuanced and depends on several factors, including the users' comprehension of the technology and their pre-existing trust in centralized authorities. Therefore, the project underscores that the path to instilling trust in SSI systems requires a comprehensive communication strategy that goes beyond the technology itself. Understanding and trust are deeply intertwined, and users may actually exhibit a higher level of trust in centralized authorities that issue and store their data if they have a clearer understanding of these centralized systems. The familiarity with traditional authorities can breed a sense of comfort, especially when compared to novel technologies like SSI. Therefore, the **communication strategy must not only focus on the benefits of SSI but also on demystifying the technology, addressing any misconceptions, and clearly articulating the advantages to gain user confidence.**

The project emphasizes that the term "self-sovereign identity" alone is not sufficient to win the trust of potential users. Instead, there is a pressing need to delve into detailed explanations of the gains and advantages associated with this novel paradigm. Users must be provided with a clear understanding of how SSI empowers them, enhances security, and provides greater control over their digital identity. This educational aspect is pivotal in bridging the comprehension gap and fostering trust in a technology that may, at first glance, seem complex or unfamiliar. Furthermore, the project recognizes that gaining trust is a process that extends beyond the mere adoption of decentralized systems. It involves ongoing engagement, active communication with users and stakeholders, and a commitment to transparency. Addressing concerns, acknowledging potential pitfalls, and continuously updating stakeholders on the technology's progress contribute to building a foundation of trust that goes beyond the initial adoption phase.

6.1.3.4 Usability as cornerstone

Is usability something that pertains to ethics? In some sense, as it directly influences the reactions, the acceptance, the outcomes of products and services, it may be. If something is not usable, or too difficult to be accessed by everyone, it could end in discrimination or even in unwanted usage The consideration of usability within the IMPULSE project elevates it to a status of paramount importance, prompting contemplation on its ethical dimensions. Usability is not merely an aesthetic concern or a superficial design element; rather, it holds profound implications for the reactions, acceptance, and overall outcomes of the products and services developed within the project. As a cornerstone, **usability is intricately tied to ethical considerations that extend beyond surface-level user interface design.**

The acknowledgment that usability can be inherently linked to ethics stems from its direct impact on the accessibility and inclusivity of the digital solutions created. It is not solely about crafting visually appealing and smoothly functioning interfaces but extends to posing essential questions about how to design for maximum inclusion. For example, the project recognizes the ethical imperative of ensuring that usability considerations are not biased or exclusionary, thereby guarding against unintentional discrimination.

Throughout the project's duration, usability has emerged as a recurrent theme, resonating in the insights provided by experts and stakeholders consulted. The consensus is clear: usability is a linchpin for achieving a successful outcome. This aligns with a broader industry trend where user experience is increasingly recognized as a critical factor influencing the adoption and effectiveness of digital solutions.

The complexities of the ethical considerations tied to usability become apparent when contemplating the consequences of a suboptimal approach. **Usability is not just about crafting an aesthetically pleasing interface; it involves thoughtful consideration of the impact on diverse user groups**. An ethical framework within usability design necessitates asking questions about the potential consequences of design choices, particularly in terms of inadvertent discrimination or unintended usage.

The project's commitment to ethical usability considerations extends beyond the immediate project deliverables. It entails a forward-looking perspective that contemplates the potential ramifications of design decisions on a broader societal scale. As technology evolves, so do ethical considerations, and the project is positioned to adapt and contribute to the ongoing discourse on ethical usability within the digital landscape. As such, some ethical recommendations pertaining to usability are included here.

6.1.3.5 Avoid the cognitive overload of the user

Usability, as a guiding principle within the IMPULSE project, goes beyond creating aesthetically pleasing interfaces and extends into the realm of cognitive considerations. Addressing the cognitive load placed on users becomes a crucial aspect of designing digital solutions that are not only user-friendly but also mindful of the mental well-being of individuals navigating complex systems. Recognizing that usability is not only about ease of use but also about avoiding undue cognitive strain, the project delves into strategies for minimizing the cognitive overload of users. Usability, in this context, translates to more than just the seamless navigation of an application or system. It involves a **delicate balance between providing users with the functionalities they need and preventing an overwhelming influx of information or decision-making responsibilities** (Guggenberger, Neubauer, Stramm, Völter, & Zwede, 2023). The project acknowledges that users can experience cognitive fatigue when confronted with continuous and demanding tasks, potentially leading to a compromised ability to make informed decisions (Ebert, Krauß, & Anke, 2023).

Striking this balance requires thoughtful design choices. One proposed solution is the implementation of a dual-mode approach, offering users both a "basic mode" and an "expert mode." In the basic mode, users are presented with simplified options, alleviating them from the burden of constant decision-making. This can be

particularly beneficial for those who prefer a streamlined experience or are less comfortable with intricate details. On the other hand, the expert mode caters to users who desire greater control and are willing to take on more decisions and responsibilities, providing a more granular and customizable experience.

The cognitive load considerations extend beyond mere functionality to encompass the broader relationship between the individual user and the institution or service provider. By recognizing that users have varying levels of comfort and expertise, the project acknowledges the importance of tailoring the user experience to accommodate different preferences. This nuanced approach aligns with a commitment to user empowerment, acknowledging that users should have agency over the complexity of their digital interactions. Ethical considerations within the usability framework are brought to the forefront as the project contemplates the potential consequences of cognitive overload. Beyond creating user-friendly interfaces, it is important to **foster a sense of responsibility among institutions and service providers to ensure that the usability of their systems does not inadvertently lead to user detriment.**

6.1.3.6 Define usability requirements that are not only general but also targeted to specific groups

When designing an eID solution one should ask which social rights and of which social groups are strengthened or on the contrary undermined by it and by the digitization of public services. Which digital technologies are best suited to enhance social rights for all EU citizens, regardless of origin or status? In this sense, social inclusion of specific groups is a major point and requires the definition of usability requirements specific to social groups, so as to integrate the needs of those that are more at risk of digital exclusion. This acknowledgement underscores the project's commitment to social inclusion, recognizing that certain groups may face unique challenges in the realm of digital identity adoption. As such, **defining usability requirements tailored to specific social groups becomes a crucial endeavor in ensuring that the benefits of digital identity solutions are accessible to all EU citizens, irrespective of their origin or status.**

This prompts the project to consider not only the general usability requirements but also those specific to certain social groups, thereby addressing the diverse needs that may arise in the process of digitizing public services. Social inclusion becomes a focal point in the discussion, emphasizing the importance of recognizing and accommodating the diverse needs of specific groups. Usability requirements tailored to these groups are designed to mitigate the risk of digital exclusion and ensure that the benefits of digital identity solutions are distributed equitably. For instance, considerations may include accessibility features for individuals with disabilities, language preferences for different linguistic communities, and interfaces that cater to varying levels of digital literacy. This targeted approach aligns with a broader understanding of digital transformation not as a one-size-fits-all solution but as a dynamic and adaptive process that considers the unique socio-cultural contexts of its users. By tailoring usability requirements to specific social groups, the project aims **to bridge the gap between technology and societal needs, thereby promoting a more inclusive and accessible digital environment.**

6.1.4 Transparency as key

Transparent communication forms the cornerstone for establishing awareness and trust within SSI systems. It is imperative to furnish users, stakeholders, and the broader public with easily comprehensible information regarding the underlying principles, functionalities, and advantages of SSI. This necessitates the demystification of intricate technical aspects, accompanied by an articulate depiction of the value proposition inherent in SSI, tailored to resonate with diverse audiences.

Furthermore, the commitment to transparency should extend to the intricate inner workings of SSI technologies. Users deserve a comprehensive understanding of how their data is managed, who possesses access to it, and the robust security measures in place. This level of openness not only provides transparency but also instills a sense of control and empowerment among users. By addressing concerns related to privacy and security, this approach actively contributes to building a foundation of trust in SSI systems.

In essence, **transparent communication acts as a bridge that connects the complexities of SSI with the broader community, ensuring that the benefits and operations of these systems are easily understood and embraced.** This transparency is not just a prerequisite for user confidence but also an essential element for the successful integration and widespread acceptance of SSI technologies.

6.1.4.1 Make the entire process transparent and accessible, involve stakeholders from the beginning and communicate all the successes but also the pitfalls

While the procedural aspects may be entirely transparent, there remains a potential gap where the intricacies of the process remain unknown to individuals. It is imperative that transparency is complemented by a robust communication strategy to successfully dispel doubts and alleviate concerns surrounding potential obscurities or concealed elements within the proposed electronic Identification (eID) solution.

As highlighted elsewhere, the communication efforts geared towards transparency must be finely tuned to cater to specific stakeholder groups. This involves **tailoring the content, style, and complexity of the information to suit the particular audience, with the aim of providing each group with the details that are most pertinent to them**. This targeted approach ensures that communication is not just transparent but also effective in addressing the unique concerns and priorities of diverse stakeholders.

In brief, the marriage of transparency and effective communication is indispensable in achieving the overarching goal of fostering confidence in the proposed eID solution. By customizing the communication strategy to various stakeholders, one can bridge the gap between transparency and understanding, thereby building a foundation of trust and acceptance for the eID solution.

6.1.5 The role of education and communication

Educational initiatives play a crucial role in increasing awareness and trust. Outreach programs, workshops, and educational campaigns can target various stakeholders, including individuals, businesses, and policymakers. These initiatives should not only elucidate the technical aspects of SSI but also emphasise its societal implications, benefits, and ethical considerations.

Empowering users with the knowledge to navigate and understand SSI contributes to informed decision-making and a more receptive user base. Educational efforts should be ongoing, adapting to evolving technologies and addressing emerging concerns to ensure a well-informed and engaged community (Ebert, Krauß, & Anke, 2023). Trust in SSI systems is inherently linked to user experience and design. User-centric design principles prioritise the user's needs, preferences, and concerns, ensuring that SSI systems are intuitive, accessible, and align with user expectations (Guggenberger, Neubauer, Stramm, Völter, & Zwede, 2023). Designing interfaces that are user-friendly and transparent infuse confidence in users, mitigating potential apprehensions about adopting new identity technologies. Additionally, user-centric design involves soliciting user feedback and integrating it into the iterative development process. By incorporating user perspectives, SSI systems can evolve to better meet the expectations and requirements of their user base, further enhancing trust.

In conclusion, increasing awareness and trust in SSI systems demands a holistic approach that includes transparent communication, educational empowerment, and user-centric design. By fostering understanding and confidence, SSI can garner broader acceptance and facilitate its integration into contemporary digital ecosystems.

6.1.5.1 Plan and activate a strong communication campaign, that targets differently different stakeholder groups

Highlighted in section 6.1.5 is the pivotal role of communication in the journey toward successful adoption, a significance underscored not only in policy round tables but especially in the initial round table detailed in D3.5.

Ensuring the effectiveness of communication is paramount, necessitating precise tailoring of efforts to diverse stakeholder groups (cfr table 2 for a list of IMPULSE project stakeholders). It is crucial not only to recognize the various stakeholders involved but also to establish clear priorities within the communication strategy. Strategic decisions, such as whether to prioritize "functional" or "operator" stakeholders, must be made to optimize the convincing process effectively.

This strategic and targeted approach is imperative, given the nuanced dynamics of different stakeholder groups. **By understanding these dynamics and aligning communication efforts accordingly, the goal is to maximize impact and secure the successful adoption of the project goals.** The emphasis on communication as a linchpin in the adoption process underscores the need for a well-calibrated and nuanced strategy, ensuring that each stakeholder group receives tailored information that resonates with their specific needs and concerns.

6.1.5.2 Consider non-traditional means of communication, for instance TED talks, serious games, etc

Introducing a new eID solution into the market presents a unique challenge due to the complexity and fragmentation of the landscape. Some countries boast mature, widely adopted eID solutions, while others may lag behind in both user readiness and public administration preparedness. Navigating this diverse terrain requires a nuanced approach, and considering the diverse levels of familiarity and readiness among potential users, adopting a non-conventional communication style emerges as a strategic choice. The rationale behind embracing a non-conventional communication style is multifaceted. On one hand, it caters to the needs of expert users who are already well-versed in existing eID solutions and are seeking more advanced features or functionalities. **The non-conventional approach can pique the interest of this user segment by offering something innovative and beyond the conventional expectations.**

On the other hand, this unconventional style holds the potential to captivate the attention of curious users who are eager to explore new possibilities (Guggenberger, Neubauer, Stramm, Völter, & Zwede, 2023). By presenting the eID solution in a novel and engaging manner, it can appeal to individuals who may not be completely ready for traditional approaches but are enticed by the prospect of something different and intriguing. Recognizing the diverse nature of the market and the varying levels of preparedness among potential users, the adoption of a non-conventional communication style becomes a strategic move. It allows for a tailored approach that can simultaneously cater to the demands of experienced users seeking advancement and capture the interest of those who are curious and open to exploration. This adaptability positions the new eID solution to make a compelling impact in a multifaceted and evolving market landscape.

6.1.5.3 Not always decentralization increases trust

Not being used to the concept of decentralization and to its advantages people may not understand it; and if centralized identity is delivered from a centralized authority that people trusts while decentralized identity services are provided by an obscure company powered by an obscure technology, people may trust the centralized one more (Giannopoulou, 2023). Decentralization is a positive factor for adoption only when and if accompanied by knowledge and communication. The added value must be clearly conveyed before being appreciated and accepted.

The recognition that decentralization does not always inherently creates trust underscores the need for a strategic communication approach. **When individuals are unfamiliar with the concept and its advantages, there is a risk that they may not fully comprehend its potential benefits**. Moreover, if centralized identity services from a trusted authority contrast with decentralized identity services offered by an unfamiliar entity utilizing obscure technology, the trust inclination may lean towards the centralized option.

Crucially, **decentralization becomes a positive catalyst for adoption only when accompanied by knowledge and effective communication strategies** (Guggenberger, Neubauer, Stramm, Völter, & Zwede, 2023). Simply put, the inherent value of decentralization must be clearly conveyed for it to be appreciated and accepted. This requires a concerted effort to educate users on the advantages and functionalities of decentralized identity solutions.

Therefore, the success of decentralized identity adoption hinges on demystifying the concept and fostering understanding through robust communication. By conveying the added value of decentralization transparently, individuals can make informed decisions, leading to a more receptive attitude towards decentralized identity services (Ebert, Krauß, & Anke, 2023). Thus, the emphasis must not only be on the technology itself but on the communication strategy that bridges the understanding gap and cultivates trust in decentralized solutions.

6.1.5.4 Train the users, transform them into evangelists

Another useful strategy is to involve citizens in the testing phase, organizing tests in a non-traditional way, letting targeted groups to test and use the application in advance and letting them communicate it to fellow citizens. Traditionally, testing has been a technical evaluation, but the proposal here is to redefine this process. By involving citizens in a non-traditional testing approach, a dynamic shift occurs. Targeted groups become early adopters, gaining access to and experiencing the application firsthand.

This unique testing paradigm serves multiple purposes. Firstly, it fosters a sense of inclusivity, making users active participants rather than passive recipients. Secondly, it allows for the identification of practical nuances and user-specific insights that might not emerge through conventional testing. These insights are invaluable in refining the application to better meet user needs.

Moreover**, by enabling these targeted groups to communicate their experiences to fellow citizens, a powerful form of grassroots advocacy is established.** Personalized testimonials and real-world experiences

often resonate more strongly with the wider audience than traditional marketing methods. Peer-to-peer communication not only builds trust but also generates a ripple effect, influencing a broader demographic. This approach not only improves the application through real-world feedback but also harnesses the power of user advocacy to drive widespread acceptance and adoption within the community.

6.1.6 Data governance and privacy

Extraterritorial conflicts arising from different values and regulations can hinder global AI governance cooperation. Also, escalatory narratives, driven by the competition for AI supremacy, may undermine collaborative efforts (Robert, Hine, & Floridi, 2023). Therefore, collaborative efforts are crucial for effective global AI governance, requiring bridging divides between countries and involving various stakeholders. Digital sovereignty is contextual and varies between regions, such as China and the EU, reflecting different policy objectives (Robert, Hine, & Floridi, 2023). **They emerge challenges in applying competition law to the digital sphere, especially with the impact of pricing algorithms and digital ledger technologies** (Alongi, 2023). So, understanding the diverse interpretations of digital sovereignty is essential for developing context-specific solutions.

6.1.6.1 Be completely transparent regarding personal data usage

Concerns regarding the usage, the storing and the transfer of personal data emerged multiple times during all the occasions in which stakeholders have been consulted**. The entire process of data storing, usage and sharing must be made transparent.** The user must know where personal data are stored and by whom, and who is going to access and use them.

6.1.6.2 Be clear about consent limits

SSI is based on the principle of the consent, freely given by the user, to the access and usage of his/her personal data. But not every transaction can be based on consent. For instance, when interacting with a public administration, personal data access is not based on consent but rather on regulations. So **it's deceiving to convey the message that the user can and must give consent prior to data access and usage**, but it's certainly fair and desirable that the user knows at least who has accessed to his/her data and for what purposes.

6.1.6.3 Persistent identity and unique personal identifiers are a concern

As outlined in the deliverable D3.3 there is ample debate in the scientific and policy community whether digital identity should be persistent or not and about the opportunity of attaching to each user a permanent, unique identifier. This last, albeit having many possible advantages increases enormously the control and monitoring potential of an eID solution and increases the related concerns. For these reasons, it would be better to avoid, albeit technically possible, to enforce unique persistent identifiers on digital identity solutions. Following these debate the latest version of eIDAS 2.0 does not include provision regarding unique persistent identifiers, but neither includes an explicit prohibition. This leaves discretion to each single country whether to adopt them or not for their digital identity solutions. Concerns have been raised (see D3.6) also about the decision to unite identification and wallet functionalities, that according to some voices should be kept separated. **A truly delicate balance between rights of the society (accountability) and rights of the individual (privacy) must be sought after** and reached and the design choices behind which approach to eID to adopt lie at its center must be made explicit.

6.1.6.4 Explore the legal and ethical implications of the use of AI into identification

Inside the IMPULSE project AI is used only for the identification phase, to match people selfies with their official (on physical ids) picture and biometric data are stored only on people's devices. So it's a quite limited use. But the possibilities of intertwining artificial intelligence and identification are much ampler: biometric technology could identify a person by her behavior or by the way she moves or talks, artificial intelligence could generate accurate fake identities to be used in the digital world, or even steal someone's identity pretending to be that person with all the connected possibilities. Data about the behavior of a person could be easily and quickly analyzed to derive conclusions from them. The online and offline movements of anyone could be tracked and used. "Echo chambers" could be generated that combined with the widespread digitization of the society and with the massive use of (trackable) digital identities could lead to really dangerous manipulative options available to ill-intentioned individuals or governments. These aspects should be addressed from a regulatory perspective, prohibiting those applications of AI technology inside matters related to identification that are found to be more dangerous for the society and for the rights of the individual. This is the approach the AI act is following, but **the relationship between AI and identification should be**

more thoroughly addressed as there may be AI applications that are not considered high risk but that in combination with identification technologies so become.

Table 5 - ethical and legal recommendations

Recommendations regarding ethical and legal issues				
Factor	**Stakeholders**	**Barriers**	**Main issues**	**Recommendations**
Technology systems are value laden **Sec. 6.1.1.1**	Functional Negatives Regulators Experts	Innovation Process	A technology (in this case an eID solution) can bring with it and convey – unknowingly – an entire set of values, that must be controlled	Make explicit the value set, operate with an ethics by design perspective, be sure that the values conveyed are compatible or coincident with the desired value set
Educational potential of eID solutions **Sec.** 6.1.1.2	Functional Regulators Experts Political	Innovation Process	Since technology is value laden it also has an educational potential, that can be exploited	Exploit the educational potential of eID solutions to enhance in citizens the perception of fundamental values
Inclusion often overlooked or not approached in the right way **Sec.** 6.1.1.3	POL/SPO/NEG/RES/ REG/DEV Regulators Responsibles Political Sponsors Developers	Interaction Innovation Process	Often inclusion is added when the design phase has already ended or is already advanced	Consult dedicated stakeholders, include them in the design team, inclusion should not be an add-on but an essential part of the design
Persistent identity and privacy concerns **Sec.** 6.1.6.3	Financial Political Negatives Decisionmakers	Innovation Contextual	The possibility of attaching to eIDs a persistent identifier, even though not mandatory, it is still available	Act on the regulatory side, deciding what is the approach to be taken. Be transparent with users about the consented uses and the possible scenarios
Risk of broadening the digital exclusion **Sec.** 6.1.1.4	Regulators Political Negatives Decisionmakers	Process Innovation Process	Some people and social groups are already digitally excluded or at risk of being so. A wrong policy with eID could worsen this situation	Adopt introduction paths differentiated by countries and social groups, perform an accurate analysis to have a clear picture of the situation and understand how to avoid broadening the digital exclusion
Risk of increasing the burden and the cognitive overload of citizens Sec. 6.1.1.7 Sec. 6.1.3.5	Regulators Functional Experts Decisionmakers	Innovation Process	Users are faced with too many choices, they are considered responsible of the protection of their data and of the consents they give. This is not fair, they should be protected from what is considered an illicit or wrong use of their data	Decide on the basis of citizens fundamental rights what can be and what cannot be done with their data and then enforce the decision without forcing people to decide each time; implement a basic and an advanced solution, where with the advanced solutions people have more possibilities but also more choices to make

Identity should be independent from the system used to ascertain it Sec. 6.1.1.6	Regulators Political Decisionmakers	Process Contextual	If the eID solution becomes the only or the preferred way to ascertain identity what happens in case of digital exclusion or of system failure?	eID should remain alongside other already existing solutions as one of the ways, but not the unique one, to ascertain identity, that remains proper of the individual
Mistrust generated by the use of biometric identification Sec. 6.1.2.3 Sec. 6.1.2.4 Sec. 6.1.2.5	Regulators Responsibles Functional Decisionmakers	Innovation Contextual	Biometrics and in particular facial recognition is becoming one of the main way to ascertain the identity but raises many privacy and control concerns	Make clear the limits of the use of biometrics, act on the regulatory side, release other less impacting systems that make use of the same technology to let people become accustomed to it
Trust as a fundamental element for an eID solution successful outcome Sec. 6.1.3.2	Operators Responsibles Functional	Innovation Process	Of course trust has a strong influence on the propensity to adopt. From an ethical point of view it is necessary to highlight how it may depend on issues such as transparency but also on less obvious factors such as the general welfare approach of a country	To achieve the objective of increasing trust (in this case in the proposed eID solution) an holistic approach should be taken, considering also factors that do not seem to have a direct relationship with eID
SSI, decentralization and their relationship with trust Sec. 6.1.3.3 Sec. 6.1.5.3	Regulators Responsibles Functional Decisionmakers	Innovation Process	SSI and decentralisation, thanks to their focus on personal data protection, seem to be “magic items” that automatically can increase trust, but that it’s not always the case	A strong communication action is needed to obtain the desired effect, explaining in detail the characteristics and the effects of both actions, that may be completely unknown to citizens
The importance of creating a favourable environment for the introduction of an eID solution Sec. 6.1.1.5	Regulators Responsibles Functional Sponsors	Organizational Innovation Process	Awareness is fundamental for the positive introduction of an eID system. One obvious move to foster it is communication but other actions, like co-creation and stakeholders involvement in each phase, have a great potential in this regard	exploit the design and the development phases of an eID solution to foster awareness in the main stakeholders and to generate interest and a positive approach.
Usability is not an absolute concept but is dependant on context and on social groups and stakeholders Sec. 6.1.3.4 Sec. 6.1.3.6	Developers Responsibles Functional Sponsors	Process Innovation Process	Usability has been identified as one of the key elements for the successful outcome of an eID solution. Unfortunately, a unique solution for each country and social group would not be feasible	Analyse each country and its social groups, elaborate targeted solutions that answer to the needs of different stakeholders and social groups, with the objective of decreasing the digital exclusion risk

Transparency should be a process rather than a static set or requirements Sec. 6.1.4.1 Sec. 6.1.6.1	Developers Responsibles Functional Sponsors Experts	Interaction Process	Transparent communication serves as the bedrock for building awareness and trust in SSI systems. Users, stakeholders, and the wider public must be provided with clear and accessible information about the principles, functionalities, and benefits of SSI as well as about the data handling	It isn't sufficient to elaborate a static set of requirements: each step of the process should be made transparent and at each step it is necessary to work with stakeholders and to target at them the communication actions
The role of communication and how to communicate effectively Sec. 6.1.3.1 Sec. 6.1.5.1 Sec. 6.1.5.2	Developers Responsibles Functional Operators	Interaction Innovation Organizational	Usually projects communicate only when the project ends, but in case of eID this isn't a win strategy.	It is necessary to communicate at each step, elaborating targeted campaigns, and making use of non-traditional means like serious games, TED talks, educationals, etc
Users over burdened with responsibilities Sec. 6.1.5.4	Regulators Responsibles Functional	Interaction Process	In SSI approaches, but also in other areas not related to identity, users are burdened with the weight of continuously taking decision regarding their privacy and the use of their data. Is this approach ethically sound?	People should not be forced to assume the responsibility of the protection of their data, what is considered wrong or unfair or dangerous for the citizen should be banned from a regulatory point of view
Concerns about personal data sharing and usage Sec. 6.1.2.1 Sec. 6.1.2.2	Developers Responsibles Functional Political Negatives Decisionmakers	Interaction Innovation Process Contextual	This is one of the most common concern and one that should be answered in detail. The possibility to use persistent identifiers remains and raises much debate.	Users should have access to who and how will use their data and where they will be stored. Particular concerns derive from the use of biometric identification and of its possibilities of tracking the individuals throughout their life and from the possibility of making the identity persistent, trough an identifier. These should be regulated
The limits of consent and of consent management Sec. 6.1.6.2 Sec. 6.1.6.3	Developers Functional Regulators	Contextual Process	Consent management is one of the central points of SSI and certainly it is of IMPULSE. Users should be made aware of the limits of consent management	Not all data exchanges can be subject to consent. Users should know when they are asked for a consent and when they can simply access the list of entities that accessed his data and for what purposes. It would be dangerous to make people believe that just anything is subject to consent

Dangers of AI as a mean of identity verification and the need for a regulatory control Sec. 6.1.6.4	**Developers** Responsibles Functional **Negatives Decisionmakers**	Innovation C**ontextual Process**	AI inside eID projects is often used in combination with biometric identification. Obviously, the possibilities are endless: they must be attentively examined and tackled	The online and offline movements of anyone could be tracked and used. "Echo chambers" could be generated that combined with the widespread digitization of the society and with the massive use of (trackable) digital identities could lead to really dangerous manipulative options available to ill intentioned individuals or governments. These aspects should be addressed from a regulatory perspective

6.2 Socio-economic

6.2.1 Introduction

Developing and introducing an eID system into a society can be considered from a double-sided point of view:

- From the one hand, it must be considered the factors, external to the solution and dependent on the society characteristics, that affect the acceptance of the proposed solution
- From the other hand, the introduction of a certain eID system into a society may have on its turn effects that should be considered when formulating recommendations

For this reason, this section will consider first the socioeconomic factors that have an influence on the introduction of an eID system, but after having done that it will also take under examination what could be the impact of the introduction of such a system and whether the proposed solution (the IMPULSE eID management) could have positive effects on some issues identified during the present analysis.

Most of the results and considerations that will find place in this section derive from the work conducted in the context of the work packages 4 and 7 of the IMPULSE project (D4.1 v1 and v2 and D7.1 v2 and v3) but some aspects have also been touched during the two policy round tables (D3.5 and D3.6).

6.2.2 Main external factors impacting an eID project

An external factor is by definition an element that does not derive from intrinsic characteristics of the project but on the context in which it is developed and introduced. For instance, while an internal factor could be the sufficient or insufficient funding, an external factor could be represented by the regulatory body of a country or by its digital infrastructure.

The main external factors identified during the project are the following:

- Regulatory bodies
- Local policies, in particular with regard to eID and digitization
- Public administrations' resistance to change
- Availability of online public services
- Economic growth and solidity
- Digitization and digital exclusion rate of a country
- Competition, overlapping projects, already existing eID systems
- Interoperability with existing systems and technologies
- Level of trust in government
- Level of trust towards technology in general
- Level of trust towards the technologies that are specific of that eID project (e.g. blockchain, biometrics, artificial intelligence, etc)

- Alphabetization and instruction level of a country's population
- Uniformity or on the contrary fragmentation of a country with respect to different levels (city level, local level, national level)

In the following table, each factor will be taken into account, highlighting the possible recommendations that could be formulated as a consequence of the lessons learned during the project's implementation

Table 6 – external factors recommendations

			Recommendations regarding external socio-economic factors	
Factor	**Stakeholders**	**Barriers**	**Main issues**	**Recommendations**
Regulatory bodies	Political Responsible Decisionmakers Experts	Interaction Contextual	The differences between countries and the excessive rigidity of certain laws and regulations have been indicated as one of the major factors impacting the success of any eID project	Make an attentive analysis of the regulations and laws in force in a certain country, do not underestimate the impact that this factor may have, work with policy makers to understand whether some regulations can be changed and/or improved, work till the design phase to adapt the project in such a way that it is able to overcome or successfully face the possible limitations due to this factor; review not only laws about eID but also the ones that regulate digital governance, open data, public sector reform, AI, cybersecurity. Digital identity is a combination of all the above elements.
Local policies, in particular with regard to eID and digitization	Political Responsible Decisionmakers	Innovation Organizational Process	Local policies may represent the line between successful introduction of an eID project and its failure. They may cover further aspects than the pure regulatory bodies and laws and can also more easily adapt to the changed situations.	Analyse the policies of the most successful countries with respect to digitisation and reduction of the digital exclusion (c.f.r D4.1 v2), work with policy makers of interested countries to implement the needed actions. A choice should be undertaken (c.f.r D6.2 v2) whether to focus on "beginner" countries or on "mature" countries (with respect to digitization and to eID usage) since their needs are extremely different and so should be the approach in developing and introducing an eID solution
Public administrations' resistance to change	Functional Political Regulators Hired Consultants	Contextual Process	The resistance to change is present both at the individual and at the collective (group, organization, structure) level. Those may be due to cultural reasons but	Appoint a group of people internal to the public administration with the sufficient authority to evangelize and if necessary enforce the needed changes; identify the objective issues (e.g. not sufficient technological equipment) and understand

			also to objective limitations.	whether and how to mitigate them
Availability of online public services	Functional Financial Operators Developers	Innovation Organizational	The possibility of accessing to a good number of high value and interesting services has been identified as one of the main reasons for adoption. The number of good online public services available is in direct proportion with the propensity to use any eID solution	Do not make the error to launch the new eID solution in the absence of a good portfolio of accessible online public services
Economic growth and solidity	Functional Financial Sponsors Developers	Innovation Organizational Process	The diffusion of an eID solution, particularly if based on the availability of devices (smartphones) and on a wide internet coverage, is dependant on economic structural conditions of a country	Consider attentively whether a certain country has the necessary infrastructural conditions, study its plan for development and the actions it is undertaking to fill the eventual gap and decide whether it is convenient to enter in that market given the actual conditions
Digitization and digital exclusion rate of a country	Negatives Regulators Experts	Innovation Process	These have been identified as one of the key factors in determining the likeliness of successful adoption of an eID solution and must be attentively considered and assessed in each country	Try to identify the factors that determine an high rate of digital exclusion and the social groups and/or country or city regions for which this factor has an higher impact; assess whether these factors can be successfully changed and the time needed
Competition, overlapping projects, already existing eID systems	Financial Sponsors Operators	Interaction Process	This issue is a fundamental one, especially in a context so diverse as the European Union with countries extremely advanced from the point of view of digitization and adoption of an eID solution	Decide the focus of your strategy and if you want to concentrate on advanced or beginner countries. In case the focus is on advanced countries, the new service must offer a true added value, something that it's not possible or not easy to have with the existing services: it may be ease of use, number of services that can be accessed with it, added functionalities (like advanced consent management), etc
Interoperability with	Negatives Decisionmakers	Interaction Innovation	Many similar eID solutions already	During all the workshops, roundtables and focus groups

existing systems and technologies	Developers	Process	exist and are in some cases widely used. The new solution must coexist alongside with the previous ones. A scenario where a person has and uses many different eID solutions according to which one performs better in a given context or for a given services must be foreseen	that have been held during the IMPULSE project always the interoperability issue emerged as a crucial one. Interoperability means coexistence of different eID solutions (that probably will continue to exist alongside the EUDI wallet) but also between different service providers and technical/hardware frameworks (in this sense the point of the constraint represented by the dominant tech companies, i.e. Apple and Google, represent a not to be underestimated aspect). To be successful any new eID solution must be kept interoperable with already existing ones and must run on all the major devices and operating systems. The extreme variety of existing devices and operating systems represents a big issue and one that must be tackled
Level of trust in government	Functional Political Regulators	Organizational Contextual	Even if the proposed eID solution is based on a decentralized SSI approach the entity that vehicles it is the central Government. Trust in government is thus essential to generate a positive attitude towards any eID solution	This is a variable that it is not immediate to take into consideration when facing the problem of the introduction of a new eID solution but that must be taken into account. Also it would be useful, if the level of trust is low, to understand the reason(s) why (e.g. scarce respect of citizens' rights) to understand if they can be transformed in advantages with the right communication action
Level of trust towards technology in general	Functional Sponsors Regulators	Innovation Contextual Process	This is or course a strong factor influencing the adoption of any technology. If combined with low digital skills and low technology affinity, these represent one of the main barriers to the adoption of an eID solution	Try to convey the new technology through services that are really appealing and working on the usability side, so as to make the new technology less "hostile"
Level of trust towards the technologies that are specific of	Functional Sponsors Regulators	Innovation Contextual Process	Here previous not so positive experiences with the same technologies (for example similar projects that failed) or the perception that	Introduce other – more simple and less critical – services based on those same technologies and that are particularly engaging, like games, to break the diffidence barrier

that eID project			these technologies – as is the case with biometrics – may put at risk values perceived as essential play a fundamental role	
Alphabetization and instruction level of a country's population	Functional Political Negatives	Organizational Contextual	Instruction level has been identified (D4.1 v2) as one of the main social factors that reduce the likelihood that people accept new eID solutions	When planning the introduction of a new eID solution do start from social groups (in this case people with an higher education level) that are more likely to have a positive stance towards the proposed technology and try to convert them in evangelists
Uniformity or on the contrary fragmentation of a country	Functional Political Negatives	Organizational Contextual	Rural areas may be extremely different from urban areas and also inside a city there may be quite different situations that determine a quite different approach towards technology in general and towards digital inclusion or exclusion in particular	A country can experience many differences in it, depending on the level (local, national…) but also for historical reasons (certain areas more developed, others less). This aspect must be attentively taken into account, because the same service cannot be delivered seamlessly at different levels. Outline and put in practice different adoption paths

6.2.3 Key factors for the social acceptance on an eID system

In the deliverable D4.1 v2 a thorough analysis has been undertaken on the factors influencing the social acceptance of an eID project in general and of the IMPULSE eID project in particular, splitting the outcomes also per pilots and country.

The main findings can be summarized as follows:

- Digital inclusion/exclusion, that is of course a complex and composed factors, is the leading factor when considering the social acceptance of an eID system
- Since age digital skills and technology affinity can be considered as key factors of digital inclusion/exclusion they play also a paramount importance role in the social acceptance of an eID system
- Other fundamental aspects are regulations and "the capability to interpret the rules in terms of multiple interests and digital needs", the "social networks" of each individual and his personal digital routines, the lack of awareness regarding the digital strategy of the government and the availability of online public services, and the corresponding ability from local public sector organizations to provide citizens with an adequate number of services and with good communication regarding to them.
- Extremely important is to identify and target special needs group of population (e.g refugees, people with disabilities, elderly people, etc) and to define a social inclusion strategy and corresponding usability requirements for these groups before analyzing the technological aspects
- Trust in government services is a major aspect, with a focus on cybersecurity and personal data usage: enhancing trust in government and in the digital services it delivers is of fundamental importance

Following a table with some possible recommendations and actions with respect to each of the points listed above

Table 7 - socio-economic factors recommendations

Recommendations regarding external socio-economic factors				
Factor	**Stakeholders**	**Barriers**	**Main issues**	**Recommendations**
Digital inclusion/ Exclusion	Functional Negatives Regulators	Organizational Contextual	Digital Exclusion appears to be one of the main factors determining the un-usage of online public services	Analyse the policies of the Nordic countries where digital exclusion seem to be lower
digital skills and technology affinity	Functional Negatives Developers	Contextual Innovation Process	Digital skills and technology affinity are in direct relationship with digital inclusion/exclusion and as a consequence with the propensity to adopt eID	Analyse the country you want to enter and if there is a low technology affinity and digital skills work on your eID solution to make it really simple and usable
Availability of online public services	Developers Political Responsibles	Organizational Innovation Process	If there aren't enthralling and/or useful services people are not going to use the eID solution; in general public services are not a good vehicle	Plan on what services make available before working on the eID solution and on the connected app
General awareness about the digital strategy of the country	Functional Political	Organizational Contextual	The country may be in evolution, its actual status could not reflect what will be the situation in the near future	Gather information about this factor before planning about how to develop and launch the proposed eID solution
Identify and target special needs group of population	Functional Political Responsibles	Organizational Contextual	The risk of creating or broadening social and/or digital exclusion areas is great	Understand since the design phase how it is articulated the social structure of the country and plan how to answer to the needs of the different groups
Economic growth and solididity	**F**inancial Political Decisonmakers	**O**rganizational **P**rocess	General aspects about the country can represent a factor of trust/mistrust	If the country is in a troubled situation or people do not trust the government to protect his rights an effort should be made to communicate how the proposed eID solution is highly advanced in protecting fundamental rights and in particular personal data usage

6.2.4 How to increase stakeholder awareness on socio-economic benefits

As it was outlined in the previous sections it is fundamental for a successful outcome that the main stakeholders are put in condition to perceive and appreciate the benefits, also economic, deriving from the adoption of the proposed eID solution. A dedicated and structured action plan is necessary to be sure to convey to the most interesting stakeholders (identified in the first phases of the project) the benefits that they may have. Of course, such benefits must have been also detected and certain aspects of the project could be given more relevance and be more thoroughly developed if they can represent a possible source of benefits for particularly interesting groups of stakeholders.

6.2.4.1 Make a good number of enthralling and useful services accessible through the new eID solution

During the first (c.f.r deliverable D3.5) and the second policy round table (c.f.r. deliverable D3.6) it was pointed out that the successful outcome and the adoption of an eID solution is not influenced by the technology (that is in some way "transparent") but by the usability and the availability of online services that can be accessed through the proposed eID solution. Paradoxically, citizens may not trust the technology but if they need (of if they like) the services, they may decide to adopt it anyway. Facebook is a great example of this behavior. In this sense, trying to introduce a new eID solution starting with public services, or only with public services, is not a good option. It is necessary to reach a "critical mass" of users and services to make a successful adoption possible.

6.2.4.2 Identify and define different social groups and target them with different communication strategies and paths of adoption

The question of communication has been sufficiently assessed in the preceding sections, so let's spend some words here on the question of the "paths of adoption", that has been suggested by a policy maker during the first policy round table. After having identified different social groups (and public administrations) characteristics and needs a good strategy is to outline a different path of adoption for each identified group, accompanying of course this action with the targeted communication plan that has been defined before.

6.2.4.3 If you have to work with the public administrations, scan their differences and their consequent different needs and difficulties and address them. A unique "take it all" strategy for all public administrations would not be effective

A question about the differences between public administrations and the necessary measures to cope with them regarding the introduction of a new eID solution has been asked during the second policy roundtable. What it emerged is that the differences between public administrations are not only a matter of how big or how small they are. Also other factors must be considered: their context, their stratification, how they evolved, how they are internally structured, how innovation is managed within them. The strategies to cope with these differences may be different (e.g. in Italy with the introduction of the SPID system it has been decided to start from the biggest public administrations and then descend towards the smaller ones) but a strategy is essential in order to reach a successful outcome.

6.2.4.4 Give the stakeholders a reason why to adopt, perceived and tangible benefits. Leverage on incentives rather than on obligations

The experts who participated in the second policy round table (D3.6) agreed that the way that leads to successful adoption of any eID solution is more easily travelled if guided by incentives rather than by obligations. In other words, thinking to force users and providers to adopt a certain eID solution may seem easier but it is not. The right way is giving users, verifiers and providers true benefits deriving from the adoption and from the use of a certain eID solution. The case of Aadhaar in India has been used to stress this point: it was not mandatory but not using it would result in discomfort and disadvantages. Act on benefits rather than on obligations is also seen as something nearer to the approach and values of democratic countries. The main benefits that have emerged through the diverse confrontations are: making things easier and quicker, improving security, privacy and control over one owned data, savings and increased revenues coming from smoother transactions. In any case, in partial contradiction with the importance that has been given by survey and workshop participants, it appears that the presence (or absence) of practical value for users is much more important than the eventual lack of privacy

6.2.4.5 Do not consider users as the only stakeholders, address also the interests of data issuers

A very interesting aspect pointed out by one of the participants to the second policy round table is that quite often the approach is extremely user centric, considering only the benefits that derive (or not) to the users from

the adoption of the proposed eID solution. But the users are not the only actors of the ecosystem. Notably, the data issuers are fundamental but are quite overlooked and the benefit for them is not clear. Also benefits for data issuers should be envisaged and strongly communicated and incentives for parties to issue data should be clearly defined

6.2.4.6 Make the business model clear and explicit to avoid unintended hidden interests

Around digital identity there is an entire ecosystem of subjects not only the citizens and the public administrations (Pierucci & Cesaroni, 2023). Private entities will need to know the economic return they may have from projects that deal with digital identity. If the business model is not made explicit it will be hidden, but will exist nonetheless. It is necessary to think about the profitability of eID initiatives for private stakeholders.

Table 8 - Recommendations regarding socio-economic factors

Recommendations regarding external socio-economic factors				
Factor	**Stakeholders**	**Barriers**	**Main issues**	**Recommendations**
Number of available service **Sec.** 6.2.4.1	Operators Developers	Innovation Organizational	Usability appears to be one of the main factors determining the un-usage of online public services	Ensure that a right amount of services are accessible through the eID system before introducing it.
Tailored adoption strategies **Sec.** 6.2.4.2	Regulators and Policymakers Decision-makers	Innovation Organizational	As well as communication, adoption paths should be adapted to different groups.	Analyse the characteristics of different social group you want to engage and propose tailored adoption paths for each of them.
Difference between public administrations **Sec. 6.2.4.3**	Political Regulators and Policymakers	Organizational Contextual	Public administrations are do not respond all in the same way to eID solutions.	Consider specificities of local public administrations to understand how they could react to the introduction of the eID system.
Perception of tangible benefits **Sec. 6.2.4.4**	Financial Responsibles Decision-makers	Organizational Contextual	Adoption of eID systems strongly depends on the users' perception	Use incentives rather than obligations, to make users perceive the eID as an opportunity and not as a problem.
Identify and target all the stakeholders Sec. 6.2.4.5	Responsibles Advisors	Process Organizational	eID success and adoption do not depends only on users	Understand since the design phase which stakeholders are involved besides users, and consider strategies for all of them.
Transparency of the business plan **Sec. 6.2.4.6**	**Financial Political Sponsors**	**Innovation Process**	Opaqueness about economic interests involved in the implementation of the system result often in a luck of trust	It should be stated very clearly who will benefits economically from the implementation of the system and in which ways.

6.3 Standards

6.3.1 Introduction

Standardization plays an important role in the IMPULSE project (1) to complement the state-of-the-art analysis with relevant standards and ongoing standardization activities, and (2) to foster the dissemination and exploitation of project results through the contribution to standardization. The first activity was conducted in task 3.4. *Analysis of existing relevant standards, and related impacts and implications*, which results are also summarized in a scientific paper (Lindner et al., 2023). The objective of this task was to create a well-grounded documentation of the current standards and standardization documents related to the IMPULSE project. The second activity refers to task 7.6 - *Initiation of standardization activities* which is part of WP7 – *Innovation and exploitation management, dissemination and communication*.

In order to understand the processes of standards development, it is important to distinguish between formal and informal standards as well as standards and specifications. Standards are developed within the formal standardization system (e.g., ISO, IEC, DIN), where all interested parties must be part of the development and agree to the final content, so-called consensus. The development time is about 3 years. In comparison, specifications can be developed in less time and in two different ways. Within standardization committees a Technical Specification (TS), addressing work under development or which can be in future the basis for a standard, and Technical Report (TR), containing supporting information such as data from a survey or a gap analysis, can be developed. Outside the standardization committees, so-called Workshop Agreements (CWA/IWA) can be developed, which respond to urgent market requirements and are not following the committee structure (ISO, 2024). Furthermore, informal standards developed in a closed body of experts, where not all interested stakeholders are involved. The major difference between the formal and informal standards are the level of consensus and the developing time (see Figure 3).

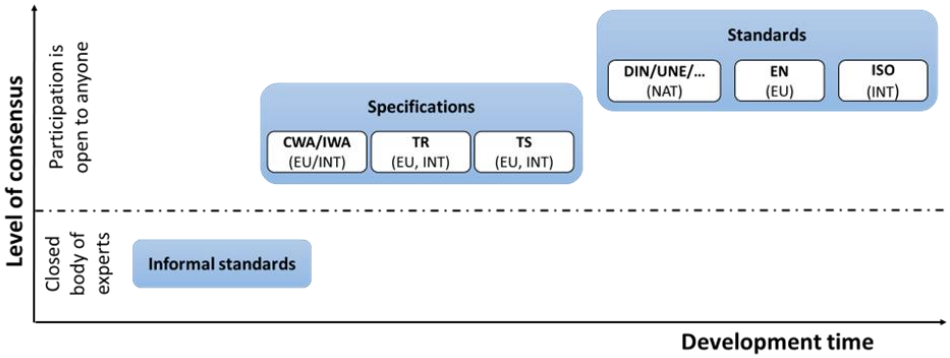


Figure 3 - types of standardization documents

Furthermore, standardization provides several benefits for the society, such as supporting innovations, efficiency and quality, facilitating competitiveness and simplify trade, as well as boosting confidence and make products safe and sustainable (CEN & CENELEC, 2024)

6.3.2 How to identify relevant eID standardization activities

The IMPULSE project identified in total nine standards, which are highly relevant for the projects' solution and its future application. These standards covering with blockchain, biometrics, eID, artificial intelligence and information technology the main project topics, are:

- CEN/TS 16921 Personal identification - Borders and law enforcement application profiles for mobile biometric identification systems
- DIN SPEC 4997 Privacy by Blockchain Design: A standardized model for processing personal data using blockchain technology
- ETSI GR SAI 001 V 1.1.1 Securing Artificial Intelligence (SAI) - AI Threat Ontology
- ETSI GR SAI 002 V 1.1.1 Securing Artificial Intelligence (SAI) - Data Supply Chain Security
- ETSI TS 119 182- 1 Electronic Signatures and Infrastructures (ESI) - JAdES digital signatures - Part 1: Building blocks and JAdES baseline signatures

- ISO/IEC 20889 Privacy enhancing data de-identification terminology and classification of techniques
- ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements
- ISO/IEC 30107 series Information technology — Biometric presentation attack detection
- UNE 71307-1 Digital Enabling Technologies - Distributed Identities Management Model on Blockchain and other Distributed Ledger Technologies. Part 1: Reference Framework

The identification of standards can be conducted in different ways. The following standards search databases and websites are recommended:

- ISO Online Browsing Platform - https://www.iso.org/obp/ui
- IEC Webstore - https://webstore.iec.ch/advsearchform
- CEN and CENELEC - https://standards.cencenelec.eu/
- National websites, e.g., DIN - www.din.de
- Standards database, e.g., NATUS - https://www.beuth.de/en/standards-management/nautos

Hereby it is important to define in advance a set of search terms to identify all possible relevant standards. Afterwards, this more complete list needs to be analyzed for the relevance of each standard to the project. Hereby an analysis of the occurrence of the search term in the title, keywords and abstract (which are always provided in the above-mentioned websites) could give an initial indication whether the standard may be of interest or not. Furthermore, an in-depth analysis of the identified standards by the research and technical partners of the project enhances the awareness of the existing standards in their field of work and ongoing standardization activities. For example, the project partners became aware of the UNE 71307-1 standard from the Spanish standardization organization, which built the basis for a future collaboration. It is also of high relevance to share the results of the standards analysis with the project partners and beyond the project (e.g. on the project website (IMPULSE, 2024); Difficulties in the standards search are the number of standards initially identified, which can be quite high due to the search terms chosen, to find the exact needed standard, which in some cases not exist yet, or the potential low interest of project partners in contributing to the standards analysis.

6.3.3 Identification of IMPULSE standardization potentials

The IMPULSE project identified during the two standardization potential workshops several ideas that can be transferred from the IMPULSE project to standardization. In summary, the following two standardization potentials merged from these workshops and exchanges in the project.

- Application of AI and Blockchain in Used Cases - Identity Management in Public Services
- Consent Management for eID Solutions

More information on the identification of standardization potentials can be reviewed in deliverable D7.15 *Overview of conducted standardization activities*. Due to the variety of ongoing standardization activities that relate to these topics, the project decided to directly interact with the standardization committees to push forward the standardization potentials.

The process of identifying the standardization potential also relates to the review of the end-user needs, which can be different from project proposal to implementation. Therefore, a project should re-assess the end-user needs and the envisaged project results. This approach can also be called demand-side. In addition, the project should check whether the existing standards are already fulfilling these needs or address the project solutions. This part can be called supply-side. When comparing the demand and supply side, potentials for standardization can be identified (Lindner, Hernantes, & Sarriegi, 2018).

Difficulties in the identification of standardization potentials could be that the project does not know if a certain project result can be transferred into standardization or that sufficient resources for standardization are lacking. In IMPULSE, the identification of standardization potentials was not difficult, but due to the progress of the development of the project solutions and the limited capacities to support the standardization tasks, more advanced contributions such as the development of a standard out of the project results could not be achieved.

Nevertheless, it was seen that the best option to foster the dissemination of IMPULSE results to standardization was via direct participation in the standardization committees (see next section).

6.3.4 How to engage with standardization

There are different possibilities to engage with standardization in research projects. During the identification of standards, the project already identified the relevant standardization committees on different level (i.e. national, European and international), which were:

- ISO/TC 307 - *Blockchain and distributed ledger technologies*
- CEN-CLC/JTC 19 - *Blockchain and Distributed Ledger Technologies*
- CEN/TC 224 - *Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment*
- UNE CTN 71/SC 307 - *Blockchain and distributed ledger technologies*

In these committees the standards relevant for IMPULSE are developed. In order to provide input to these committees, there are different possibilities. The first one is to develop a CEN/CENELEC Workshop Agreement (CWA). For this, a project plan with scope, elements and contributors of the envisaged document has to be developed, which is publicly available for 30 days to gather potential comments and contributors. The positive aspect with a CWA is that the project can completely decide the way of working and can develop the document within a short time frame, e.g. 6 months. The resulting CWA can be directly proposed to the relevant standardization committees for uptake.

The second option is direct interaction with the standardization committees. Here it is possible to either propose a new work item for standardization, which can lead to the development of a standard, a Technical Specification or a Technical Report on either national, European or international level. However, this may be difficult if you do not have project partners directly involved in the standardization committees, as the processes and consensus building may be long and difficult. However, in the case of IMPULSE, the Spanish project partner Gradiant became a member of the UNE CTN 71/SC 307 - *Blockchain and distributed ledger technologies* to directly support the development of the UNE 71307 standards series with input from IMPULSE. (UNE, Spanish Association for Standardisation - CTN 71/SC 307 - Blockchain and distributed ledger technologies, 2024) (UNE, 2020)

Another option is a project liaison with the relevant standardization committees on European or international level to provide feedback to ongoing standardization activities in these committees. The IMPULSE project decided to set up a liaison with the two working groups 18 on *biometrics* and 20 on *the European Digital Identity Wallets* of the CEN /TC 224 - *Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment.* This committee has the scope to develop standards for strengthening the interoperability and security of personal identification and its related personal devices, systems, operations and privacy in a multi sectorial environment (CEN, 2024). It covers:

- Operations such as applications and services like electronic identification, electronic signature, payment and charging, access and border control;
- Personal devices with secure elements independently of their form factor, such as cards, mobile devices, and their related interfaces;
- Security services including authentication, confidentiality, integrity, biometrics, protection of personal and sensitive data;
- System components such as accepting devices, servers, cryptographic modules.

During the liaison with this standardization committee, IMPULSE partners got insights about the development of new standards relevant for the project, such as CEN/TR *17982 European Digital Identity Wallets standards Gap Analysis* (CEN, 2023a) or CEN/TR 18030 *Personal identification - Biometrics - Overview of biometric verification systems implemented across Europe* (CEN, 2023b). Furthermore, the project partners were able to comment on other standards under development and thus to provide input with the IMPULSE point of view.

Difficulties in such engagement with the standardization system are to get the support of the right project partners to the specific items of the standardization committees and to attend actively the meetings of these committees. A possible disadvantage of a liaison is that not the project results might only be very limited be transferred into standardization, as the standardization committees have their work programme and limited resources. In comparison to the development of CWA, as a softer fast-track version of standardization, the contribution to standardization is directly happening without loose of information. However, afterwards it is of relevance to promote the CWA actively in the relevant standardization committees. Therefore, a combination of both, a CWA development and a liaison, may be the best solution to transfer project results into standardization and to foster the sustainability of project results, which are through the global availability of standards and the continuous revision process of each document after several years ensured.

7 Conclusions

The IMPULSE project has embarked on an extensive and collaborative exploration of digital identity and wallets, employing a co-creative and inclusive methodology that actively engaged stakeholders throughout the project's life cycle. This deliverable systematically delves into a range of crucial aspects, drawing evidence from internal project activities and an extensive review of pertinent scientific literature. This deliverable not only serves as a compendium of valuable findings but also tailors recommendations for policymakers and stakeholders. Its scope extends beyond the immediate realms of digital identity and wallets, touching upon broader subject areas like innovation and change management in public services, technology acceptance, regulatory aspects influencing technological innovation, and the nuanced nature of identity with itssocietal implications.

A particularly thoughtful approach is adopted in understanding the term "disruptive" within the IMPULSE context, going beyond technological considerations to encompass how digital identity management is treated and regulated. The document thoroughly explores disruptive technology and processes, emphasizing their social, ethical, legal, and socio-economic impacts rather than just industry disruptiveness. Drawing inspiration from Christensen's seminal work (1997), the document characterizes disruptive technology as having the potential to fundamentally change established technologies, rules, business models, and societal norms. It highlights the intriguing fact that disruptive technologies may initially be perceived as inferior but later generate new user needs, ultimately reaching a larger market. The distinction between first-order and second-order disruptions, as elucidated by Schuelke-Leech (2018), provides a nuanced perspective that aligns closely with the transformative nature of the IMPULSE project. Its disruption goes beyond the mere use of technologies like blockchain; it introduces relevant changes to social structures, processes, roles, and user expectations.

Moreover, the document underscores the confluence of disruptive effects arising from both the proposed eID solution and the evolving regulatory framework, particularly the eIDAS Regulation. As digital identity plays an integral role in interactions across platforms, the eIDAS Regulation, established in 2014, has brought transformative effects to the European digital market. The subsequent Proposal for eIDAS 2.0 reflects the ambitious European Commission's goal to deliver a secure and trusted digital identity for all EU citizens. The in-depth analysis of the eIDAS Regulation and the Proposal underscores their pivotal role in shaping the digital identity landscape. Anticipated transformative changes are expected with eIDAS 2.0, featuring the European Digital Identity Wallet.

Section 5 of this document delves into potential barriers and risks to the successful implementation of a digital identity system, drawing on insights gleaned from the IMPULSE project. Acknowledging the dual role of the regulatory framework as both a facilitator and potential impediment, the transformative nature of introducing digital identity into society is keenly recognized. The IMPULSE project, with its focus on digital identity management in public services, offers valuable outcomes from pilot observations, policy round tables, a citizen survey, and theoretical research. Identified barriers are thoughtfully categorized into organizational, interaction-specific, innovation characteristics-related, contextual, and process stage-related aspects. This categorization, inspired by the work of (Cinar, Trott, & Simms, 2019)serves as a robust foundation for subsequent sections, linking each barrier to its category and potential risks. These categorizations contribute significantly to a comprehensive understanding of challenges in digital identity implementation, intricately connecting with recommendations and lessons learned in the subsequent sections. Subsequently, the document explores key barriers and proposes mitigating actions to facilitate the adoption of a digital identity system, focusing on specific challenges and potential solutions.

Moving on to Section 6, the document provides someinsights into the challenges and opportunities associated with the introduction of an eID system. This section outlines key recommendations and lessons learned, with a specific focus on ethical and legal aspects, socio-economic considerations, and the importance of standards. Aligned with the European Commission's eIDAS and eIDAS 2.0 Regulations, the IMPULSE project strongly advocates for a Self-Sovereign Identity (SSI) approach. This approach aims to empower citizens in managing their personal data, with a significant emphasis on ethical considerations outlined in project deliverables. Addressing conflicts between individual rights and societal needs, this section underlines the crucial importance of ethical and legal considerations, especially concerning biometric data. The project further

highlights potential vulnerabilities in European-wide SSI adoption, urging a critical evaluation of assumptions and best practices in data governance for responsible implementation.

The socio-economic aspect of implementing an eID system is a multifaceted endeavour that involves assessing external factors, societal impacts, and deriving recommendations based on lessons learned from the IMPULSE project. External factors identified span regulatory bodies, local policies, public resistance, and more, underscoring the complexity of the socio-economic landscape. This socio-economic section delves into key factors influencing social acceptance, emphasizing aspects such as digital inclusion/exclusion, age, skills, regulations, social networks, and trust in government services. To enhance stakeholder awareness, the document proposes specific actions, including making services accessible through the eID solution, employing diverse communication strategies for different social groups, addressing public administration differences, and emphasizing perceived benefits rather than obligations. Importantly, it highlights the inclusion of data issuers in the ecosystem and the need for a transparent business model.

These socio-economic recommendations are crafted to guide the successful implementation of eID systems, ensuring broad societal acceptance and tangible benefits for all stakeholders involved. Within the IMPULSE project, standardization plays a pivotal role, serving two main purposes: enriching the state-of-the-art analysis and facilitating the dissemination of project outcomes. The analysis involved a meticulous examination of existing standards, leading to the identification of nine key standards crucial for the IMPULSE solution and its future applications. Understanding the formal and informal standards, their benefits to society, and the methodology for identifying relevant eID standardization activities were key aspects of the project's approach. The project identified standardization potentials, with a specific focus on AI and blockchain in identity management and consent management for eID solutions.

In summary, the IMPULSE project, as this deliverable tried to highlight, provides a rich tapestry of insights and recommendations for digital identity systems. Its contributions span ethical considerations, socio-economic implications, regulatory landscapes, and the vital role of standards. This document shows how a project like IMPULSE not only can add significant value to the digital identity discourse but also lays the groundwork for responsible, secure, and inclusive implementations in the ever-evolving technological landscape.

References

Alkalifah, A., & D'Ambra, J. (2013). The Role of Trust in the Initial Adoption of Identity Management Systems. In H. F. Linger, *Building Sustainable Information Systems*. Boston, MA: Springer.

Alongi, L. (2023). Digital Sovereignty and Competition Law in China and in the EU. In Timoteo, Verri, & Nanni, *Quo Vadis Sovreignty*. PSSP.

Ballejos, L. C. (2008). Method for stakeholder identification in interorganizational environments. *Requirements Engineering, 13*(4), p. 281–297. doi:10.1007/s00766-008-0069-1

Bisson, D. (2021, 08 6). *Ransomware Costs Expected to Reach $265 Billion by 2031*. Retrieved from SecurityIntelligence: https://securityintelligence.com/news/ransomware-costs-expected-265-billion-2031/

CEN. (2023a). *European Committee for Standardisation. CEN/TR 17982:2023-09 European Digital Identity Wallets standards Gap Analysis.* Retrieved from https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:75912,6205&cs=10318ADE251A22A4BB8E01D58F64E8CDD

CEN. (2023b, 12). *European Committee for Standardization. CEN/TR 18030:2023-12 Personal identification - Biometrics - Overview of biometric verification systems implemented across Europe.* Retrieved from https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:69768,6205&cs=19F68939711BB6DB7303E3F41DA459D3C

CEN. (2024). *Technical Committee 224 on Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment.* Retrieved from https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:6205&cs=1E59B4D3EFD280E27AAC0C16CC13CD4FD

Christensen, C. (1997). *The Innovator's Dilemma: the Revolutionary Book that Will Change the Way You Do Business*. Boston (MA): Harvard Business School Press.

Christensen, C. (1997). *The Innovator's Dilemma: the Revolutionary Book that Will Change the Way You Do Business*. Boston (MA): Harvard Business School Press.

Christensen, C. (1997). *The Innovator's Dilemma: the Revolutionary Book that Will Change the Way You Do Business*. Boston (MA): Harvard Business School Press.

Christensen, C. (1997). *The Innovator's Dilemma: the Revolutionary Book that Will Change the Way You Do Business*. Boston (MA) : Harvard Business School Press.

Christensen, C. M. (2013). Disruptive innovation. In *The Encyclopedia of Human-Computer Interaction (second ed.)*. Interaction Design Foundation.

Cinar, E., Simms, C., Trott, P., & Demircioglu, M. (2022). Public sector innovation in context: A comparative study of innovation types. *Public Management Review*. doi:10.1080/14719037.2022.2080860

Cinar, E., Trott, P., & Simms, C. (2019). A systematic review of barriers to public sector innovation process. *Public Management Review, 21*(2), 264-290. doi:10.1080/14719037.2018.1473477

Cinar, E., Trott, P., & Simms, C. (2021). An international exploration of barriers and tactics in the public sector innovation process. *Public Management Review, 23*(3), 326-353. doi:10.1080/14719037.2019.1668470

Determann, L. (2021, 9 28). *Standardizing data-processing agreements globally*. Retrieved from IAPP: https://iapp.org/news/a/standardizing-data-processing-agreements-globally

disruptive technology. (2023, November 24). Retrieved from Oxford Reference : https://www.oxfordreference.com/view/10.1093/oi/authority.20110810104753313

DS, D. S. (2024, 01 10). *Personal identification – Biometrics – Overview of biometric verification systems implemented across Europe.* Retrieved from standards.globalspec.com: https://standards.globalspec.com/std/14628649/DSF/FPRCEN/TR%2018030

Ebert, S., Krauß, A. M., & Anke, J. (2023). Towards informed choices: A decision model for adaptive warnings in self-sovereign identity. *dl.gi.de*.

EDRI - Epicenter Works for Digital Rights. (2022, january 25). *eIDAS policy paper*. Retrieved from Epicenter Works: https://epicenter.works/fileadmin/import/eidas-policy_paper-ewedri_0.pdf

European Commission . (2023). *Europe's Digital Decade: digital targets for 2030*. Retrieved from commission.europa.eu: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

European Commission. (2014). *Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity.* Retrieved from EUR-Lex: https://eur-lex.europa.eu/resource.html?uri=cellar:6f30628d-c458-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF

European Commission. (2014). *Reports from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0290

European Commission. (2015, September 8). *COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014* . Retrieved from eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1501&from=EN

European Commission. (2020). *State of the Union Address by President von der Leyen at the European Parliament Plenary.* Retrieved from ec.europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

European Commission. (2021, June). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.* Retrieved from eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

European Commission. (2023, April 25). *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. Retrieved from ec.europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413

European Commission. (2023, May 23). *EU Digital identity: 4 projects launched to test EUDI Wallet*. Retrieved from digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet

European Commission. (2023, February). *European Digital Identity Wallets: Commission publishes first technical Toolbox towards prototypes*. Retrieved from digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/news/european-digital-identity-wallets-commission-publishes-first-technical-toolbox-towards-prototypes

European Commission. (2023). *Shaping Europe's digital future.* Retrieved from The European Digital Identity Wallet Architecture and Reference Framework: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

European Council. (2020, October 2). *European Council conclusions, 1-2 October 2020.* Retrieved from consilium.europa.eu: https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf

European Parliament . (2023, November). *European Digital Identity - Provisional Agreement*. Retrieved from www.europarl.europa.eu: https://www.europarl.europa.eu/committees/en/european-digital-identity-provisional-ag/product-details/20231116CAN72103

European Parliament and Council. (2014). *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation).* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

European Parliament, & European Council. (2023, November 8). Retrieved from Europarl: https://www.europarl.europa.eu/committees/en/european-digital-identity-provisional-ag/product-details/20231116CAN72103

Friedhoff, T., Cam-Duc, A., Ladnar, N., Stein, D., & Zureck, A. (2023). Analysis of Social Acceptance for the Use of Digital Identities. *Computers, 12*(3). doi:10.3390/computers12030051

Giannopoulou, A. (2023). Digital Identity Infrastructures: a Critical Approach of Self Sovereign Identity. *DISO 2, 18*.

Guggenberger, T., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023). T. Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Application. *Proceedings of the 56th Hawaii International Conference on System Sciences.*

Hafer, G. (2021, 3 23). *FBI: Internet Crime up Almost 70% in 2020*. Retrieved from AMAC Foundation: https://amacfoundation.org/fbi-internet-crime-up-almost-70-in-2020/

Halperin, R., & Backhouse, J. (2012). Risk, trust and eID: Exploring public perceptions of digital identity systems. *First Monday, 17*(4). doi:doi.org/10.5210/fm.v17i4.3867

Hopster, J. (2021). What are socially disruptive technologies? *Technology in Society, Volume 67*. doi:https://doi.org/10.1016/j.techsoc.2021.101750

IMPULSE. (2024). Retrieved from IMPULSE project website: http://www.impulse-h2020.eu

Ishmaev, G. (2021). Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and Information Technology, 23*(3), 239-252.

Ishmaev, G., & Stokkink, Q. (2020). Identity Managment Systems: Singular Identities and Multiple Moral Issues. *Frontiers in Blockchain, 3*(5). Retrieved from https://www.frontiersin.org/articles/10.3389/fbloc.2020.00015

ISO. (2024). Retrieved from Website of ISO deliverables. International Organization for Standardization.: https://www.iso.org/deliverables-all.html

ISO/IEC 24745:2022 . (s.d.). ISO/IEC 24745:2022 Information security, cybersecurity and privacy protection — Biometric information protection. Retrieved from https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24745:ed-2:v1:en

Khan, W., & Abideen, Z. (2023). Effects of behavioural intention on usage behaviour of digital wallet: the mediating role of perceived risk and moderating role of perceived service quality and perceived trust. *Future Business Journal volume, 9*(73).

Lindner, R., Hernantes, J., & Sarriegi, J. M. (2018). Standardization process for urban resilience. *Reframing Urban Resilience Implementation: Aligning Sustainability and Resilience.* Barcelona. doi:10.3390/IFOU2018-05981

Lukkien, B. D. (2023). Barriers for developing and launching digital identity wallets. *Proceedings of the 24th Annual International Conference on Digital Government Research - Together in the Unstable World: Digital Government and Solidarity, DGO 2023 (ACM International Conference Proceeding Series). Association for Computing Machinery* (p. 289-299). D. D. Cid.

Marsman, H. (2022). Is the Capabilities Approach operationalizable to analyse the impact of digital identity on human lives. *Data & Policy, 4*. doi:10.1017/dap.2022.37

Martin, N. (2023). The Chimera of Control. Some Critical Reflections on Self-Sovereign Identity. *Fifthteenth interdisciplinary workshop on "Privacy, Data Protection & Surveillance".* Berlin: Alexander von Humboldt Institute for Internet and Society.

Mitchell, R. K. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *The Academy of Management Review, 22*(2). doi:10.2307/259247

Pierucci, F., & Cesaroni, V. (2023). Data Subjectivation-Self-sovereign Identity and Digital Self-Determination. *Digital Society, 2*(2).

Robert, H., Hine, E., & Floridi, L. (2023). Digital Sovereignity, Digital Expansionism, and the Prospects for Global AI Governance. In Timoteo, Verri, & Nanni, *Quo Vadis Sovereignty?* . PSPS .

Rosca, V. (2017). *Exploring barriers to Mobile e-ID adoption : A government perspective on Republic of Moldova Mobile e-ID (Dissertation).* Retrieved from Umeå University, Faculty of Social Sciences, Department of Informatics: https://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-137068

Schuelke-Leech, B. (2018). A model for understanding the orders of magnitude of disruptive technologies. *Technol. Forecast. Soc. Change, 129*, 261-274. doi:10.1016/j.techfore.2017.09.033

Tsap, V., Pappel, I., & Draheim, D. (2017). Key Success Factors in Introducing National e-Identification Systems. In T. W. Dang (A cura di), *4th International Conference, FDSE. 10646.* Ho Chi Minh City: Springer. doi:10.1007/978-3-319-70004-5_33

UNE. (2020). *Spanish Association for Standardisation - UNE 71307-1:2020 - Digital Enabling Technologies. Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. Part 1: Reference Framework.* Retrieved from https://www.en.une.org/encuentra-tu-norma/comites-tecnicos-de-normalizacion/comite?c=CTN+71/SC+307

UNE. (2024). *Spanish Association for Standardisation - CTN 71/SC 307 - Blockchain and distributed ledger technologies.* Retrieved from https://www.une.org/encuentra-tu-norma/comites-tecnicos-de-normalizacion/comite?c=CTN+71/SC+307

Zwitter , A., & Gstrein, O. J. (2021). Editorial: Identity and Privacy Governance. *Frontiers in Blockchain*. Retrieved from https://ssrn.com/abstract=3906511