Impulse

Identity Management in PUbLic SErvices

D4.2 Report on the social perception and recommendations - V2

Lead Author: Thomas Jackwerth-Rice

With contributions from: Wiebke Baumann, Knut Blind, Frederik Metzger, Nicholas Martin, Liliya Pullmann

Reviewer: Francesca Morpurgo, Bertille Auvray, Giorgi Simeonov

Deliverable nature:	R (report)
Dissemination level: (Confidentiality)	PU (public)
Delivery date:	21/12/2023
Version:	2.0
Total number of pages:	52
Keywords:	digital inclusion, eID solutions, acceptance, adoption, welfare states

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

Executive summary

This study is part of the IMPULSE research project, which has developed and piloted new eID management solutions that provide users with a Self-Sovereign Identity (SSI). It proposes an innovative solution for EU citizens to manage their electronic identities and use Online Public Services (OPS) more frequently.

The main objective of this deliverable is to **identify the social and cultural factors that promote or hinder the acceptance and adoption of new eID solutions such as IMPULSE**. The study is based on Work Package 4 (WP4) of the IMPULSE project, which has analysed the social perception of eID solutions and OPS in more detail.

In addition, in relation to the six cases piloted by the IMPULSE project, our **main KPI was to identify three to five adoption factors**. The authors of this study distinguish between acceptance and adoption because this allows a systemic assessment of individual habits and perceptions (acceptance) as well as a broader analysis of the rationale why other organisations should adopt such a new eID solution, which would contribute to the uptake of such solutions.

Our study is based on a pan-European web survey, expert consultations and the results of the pilot cases conducted during the WP2 project. Our results show that important factors for acceptance are age, digital skills, technology affinity and education. We also found that the IMPULSE solution was perceived positively by the vast majority of the survey participants.

Based on our analysis of social perceptions, we concluded that other non-technical measures, such as putting more government services online, providing better information about these services, or deleting data on request, could promote digital inclusion effectively if they increased trust in OPS and made it easier to access and use them.

We also found that EU citizens from social democratic and southern European countries are least likely to be digitally excluded, while citizens from Germany and Bulgaria are most at risk. On the basis of these findings, our conclusion is that an inclusive EU digital policy could learn from the policies and institutions of the Nordic welfare states, as they may be more effective in addressing issues of both social and digital exclusion.

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	Jens HEMMELSKAMP		

Deliverable	**Number**	D4.2	**Title**	Report on social perception and recommendations - V2
Work package	**Number**	WP4	**Title**	Social and Economic Impact Assessment
Task	**Number**	T4.1	**Title**	Socio-political impact assessment

Date of delivery	**Contractual**	M34	**Actual**	M35
Status	version 1.0		☒Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)	Wiebke Baumann, Knut Blind, Frederik Metzger, Nicholas Martin, Liliya Pullmann, Diana Silvestru			
Responsible author	**Name**	Thomas Jackwerth-Rice		
	Partner	Fraunhofer ISI	**E-mail**	thomas.jackwerth-rice@isi.fraunhofer.de

Summary (for dissemination)	*The main objective of this deliverable is to identify the social and cultural factors that promote or hinder the acceptance and adoption of new eID solutions such as IMPULSE.*
Keywords	*eID solutions, SSI solutions, acceptance, adoption, survey, welfare regimes*

Version Log

Issue Date	Rev. No.	Author	Change
17/11/2023	0.1	Thomas Jackwerth-Rice	Fraunhofer ISI internal review
28/11/2023	0.2	Nicholas Martin	Chapter 5.2 on biometrics added, some minor corrections/revisions
29/11/2023	1.0	Thomas Jackwerth-Rice	Submitted for review within the IMPULSE project
02/12/2023	1.1	Review: Francesca Morpurgo	Changes in the introduction & sec. 2, minor changes in sec. 5
14/12/2023	12	Review: Federica Russo	Changes in sec. 2, minor changes in the rest of the doc.
21/12/2023	2.0	Thomas Jackwerth-Rice	Final version send to IMPULSE project coordinator for submission

Table of contents

List of figures

List of tables

Abbreviations and acronyms

DE	*Digital Exclusion*
DI	*Digital Inclusion*
DV	*Dependent Variable*
D4.1	*Deliverable 4.1*
D4.2	*Deliverable 4.2*
EFS	*Enterprise Feedback Suite*
FRT	*Facial Recognition Technologies*
KPI	*Key Performance Indicator*
eID	*electronic identity*
IMPULSE	*Identity Management in PUbLic SErvices*
IV	*Independent Variable*
NGO	*Non-governmental organization*
OPS	*Online Public Services*
PPP	Public-Private Partnerships
SSI	*Self-Sovereign Identity*
SPID	*Public Digital Identity System*
SSO	*Single Sign-On*
T4.1	*Task 4.1*
VC	*Vulnerable Citizens*
WP	*Work Package*

1 Introduction: The problem of digital inclusion in Europe

In Europe, EU Member States will increasingly deliver their services online, so access to these services will be crucial for citizens and organizations alike to benefit from public services. However, in Europe, some social groups may refrain from using public services online, which could lead to their exclusion from public services. Therefore, we believe that new technologies such as IMPULSE should be analyzed in the context of the policy issue of Digital Inclusion (DI), which takes both technical solutions such as IMPULSE, but also non-technical factors such as policies and institutions into account.

In fact, the issue of DI is one of the key objectives of the EU's Digital Strategy: Digital technologies should guarantee all citizens both equal participation in public life and the exercise of their social rights, such as work, health, privacy or public expression (EP, 2022; Mossberger et al., 2003; Renda et al., 2021; Van Deursen & Helsper, 2015). However, the below mentioned definition of DI suggests that everyone moving around Europe should be able to access and use public services online, regardless of their socio-economic status, citizenship within the EU, individual attitudes or skills (EP, 2014; Petmesidou & Guillén, 2022).[1] We therefore agree with researchers who see effective digital inclusion policies closely associated with social exclusion issues.

> *Digital inclusion is defined as "equitable, meaningful, and safe access to use, lead, and design of digital technologies, services, and associated opportunities for everyone, everywhere" (UN, living document).*

Understanding DI as closely associated with social inclusion, this study explores the **social and cultural factors which drive the users' behavior and thus the adoption and acceptance of eID solutions** for public services.[2] Given the high social and cultural heterogeneity of European welfare states, we assume that those factors of acceptance and adoption very much differ across Europe (cf. Alexopoulou et al., 2022; issa, 2022).

It is against this background that we take a critical perspective on how new technologies, such as IMPULSE, could contribute to the digital inclusion of a wide range of social groups. Indeed, based on recent research, we hypothesise that the social and cultural factors driving the acceptance and use of new eID solutions and Online Public Services (OPS) are mediated by the political systems of social inclusion, which vary across welfare regimes (Alexopoulou et al., 20-22).

Our main KPI was to identify **three to five adoption factors for each pilot case** in the IMPULSE project, based on all our research, which included a literature review (cf. Jackwerth-Rice et al., 20-23), a pan-European web survey and qualitative expert interviews. In the final section (section 7), we critically discuss the importance of non-technical factors for the digital inclusion of vulnerable social groups.

We have structured our study in the following way. First, we present our framework for the analysis of social and cultural differences in the acceptance and adoption of eID solutions in Europe (*section 2*). After the presentation of our methods and data (*section 3*), we outline the social and cultural factors of acceptance and adoption in Europe (*section 4*). In *section 5*, we assess how the IMPULSE solution might contribute to digital inclusion, while in *section 6*, the adoption factors for the pilot cases are specified. We summarize our data and draw conclusions in the final section.

[1] By 2030, at least 80% of EU citizens should be able to access public key services using digital identities.

[2] For the general differentiation of acceptance and adoption factors, see Deliverable D4.1 V1 (cf. p. 11-15). Basically, acceptance factors refer to the individual perception and the individual handling of eID solutions for online services. Adoption factors, on the other hand, refer to the institutional context that promotes digital inclusion or to organizations that provide online services, such as public authorities, municipalities, or educational institutions.

2 Political approaches to DI in Europe

Within WP4.1, one of the main objectives was the assessment of the social and cultural factors for the acceptance and adoption of new eID solutions. As mentioned above, we believe these factors are strongly linked to the political systems of social inclusion, which varies widely across European welfare states. In order to account for this heterogeneity of Europe, we distinguish four different political approaches to support social inclusion. This might then translate into different levels of digital inclusion.

Our main assumption is that the level of **digital inclusion is likely to vary considerably across EU Member States due to different policy approaches to social inclusion**. This is because the risk of both social and digital exclusion is perceived differently in these countries. In other words, our expectation is that the more EU member states invest in social inclusion, the more politics and societies are sensitive for the risks of digital exclusion.

2.1 Welfare regimes as institutional contexts of DI

Welfare regimes are designed to protect people's social rights and to ensure, to varying degrees, that individuals can maintain their livelihoods outside the labor market. This is particularly the case with regard to pensions, unemployment benefits and sickness insurance (Esping-Andersen, 1990; Kammer et al., 2012). Against this backdrop, our argument is that policies and institutions may be based on different expectations of how digital inclusion should be promoted, which are deeply rooted in the culture of these societies.

Dealing with DI refers to several aspects which are more related to the individual who is actually using a new digital technology. First, individuals must be motivated to use a new digital solution (*motivational aspects*). They must also have physical access to such technologies (*material aspects*), and they must have the skills to operate the technologies and applications (*skills aspect*). These individual characteristics are main social conditions of using new digital solutions (*usage aspect*) (Nguyen 2020; van Dijk 2005). In our web survey, we have covered these aspects with similar variables.

Other researchers point to the political system of dealing with issues of social inclusion, which differs from one welfare system to another and therefore then might have a different impact on the level of DI (Alexopoulou et al., 2022). In fact, based on the research on European welfare states, we suggest that **welfare institutions and policies influence the way in which a society perceives the risks of digital exclusion** and, therefore, the way in which policy-makers actually address these risks.

2.2 Four approaches to social inclusions (our assumptions on DI)

To this end, we have formulated four assumptions about how the level of DI differs in the European welfare states included in our study — a) social democratic countries, b) conservative countries, c) southern European countries and d) eastern European countries (Esping-Andersen, 1990; Ferrera, 1996).[3] Our assumptions are summarized in **¡Error! No se encuentra el origen de la referencia.**. We used our survey data to test these assumptions.

Welfare regime type	Dealing with social inclusion	Digital inclusion	Digital exclusion
a) Social democratic countries e.g. Denmark, Finland, Iceland	Social inclusion is based on universalistic principles of social equality e.g. in education or access to information	Strongest inclination to use OPS	Least degree
b) Conservative countries e.g., Germany, France, Austria	Social inclusion is rather based on the basis of occupational status which provide insurances for their members, countries provide good material conditions	Medium inclination to use OPS, clearly distinguishable across occupational status groups	Medium degree
c) Southern European countries e.g., Italy, Spain	Social inclusion is highly fragmented into insider-outsider segments of the labor market (e.g., corporatist income	Medium inclination to use OPS, higher for	High degree

[3] The Eastern European welfare model include countries such as Lithuania, Latvia, Estonia, Bulgaria or Romania (Lauzadyte-Tutliene et al., 2018)

	maintenance system), strong family dependency for welfare provision, weak role of the state	insiders, low for outsiders	
d) Eastern European e.g., Bulgaria	Limited government spending on social protection. States provides some support for education, but countries are typically characterized by high income and gender inequalities and less developed infrastructures	Lowest inclination to use OPS	Highest degree

Table 1 Welfare regimes included in the survey

Assumption 1: **Social democratic** countries tend to have a **universalistic approach** to social policy, meaning that social benefits are provided to citizens on the basis of their social rights as citizens (Syvertsen et al., 2014). We therefore expect to find the **lowest levels of digital exclusion** in these countries, as it is here that policymakers might most strongly be involved in the promotion of social equality in education, financial security, but also access to information, and therefore actively pursue this for the digital world (Esping-Andersen, 2015). We also expect **greater inclination to OPS** across social groups, as digital skills are promoted early in peoples' life course and more comprehensively which should reduce the risks of digital exclusion.

Assumption 2: Compared with social democratic countries, **conservative countries** tend to have a tradition of social policies that require their citizens to take more responsibility for their own social security. They also have a tendency to **reproduce social inequalities**, because social benefits are distributed less on the basis of equal treatment and universalistic principles, and more on the basis of **membership of occupational groups** that provide different kinds of insurance for their members, such as unemployment insurance or health insurance. Nevertheless, these welfare states are often leading market economies in Europe, which should provide good material and infrastructural conditions for promoting digital inclusion. Overall, we expect a **medium level of digital exclusion**. In addition, the **inclination to use government online services** might be **clearly distinguishable** between different social groups.

Assumption 3: In **southern European** countries, social inclusion is characterized by a state that plays a much weaker role than in Scandinavia or conservative countries. In addition, obtaining social benefits and levels of social security is here more dependent on insider-outsider issues, with insiders being employed for example by the state or large private companies. In comparison with social democratic countries, individuals are more dependent on large families to cover social risks, e.g. for care and child rearing (Gal 2010; Ferrera, 1996). We therefore expect a **higher value for both digital exclusion and the inclination to use OPS** than in the social democratic welfare states. Furthermore, we expect strong differences in digital inclusion due to differences in the occupational status.

Assumption 4: **Eastern European** countries are characterized by the lowest levels of government spending on social protection, but the state still supports education. These countries are also typically characterized by high income and gender inequalities (Aristei & Perugini, 2012; Lauzadyte-Tutliene et al., 2018). In addition, these countries have less developed infrastructures, such as for internet access. Thus, with such a more limited approach to social inclusion compared to the other welfare regimes, we expect these countries to have the **weakest levels of digital inclusion and inclination towards OPS**.

3 Methods and data

As part of WP4.1, we designed and carried out a pan-European web survey and conducted expert consultations in order to obtain the empirical data for our study. Both methods have already been described in D4.1 (V1). Therefore, this chapter only illustrates our data evaluation strategy, including the main variables we analyzed.

3.1 Web survey

The survey was carried out from the 5th of **May 2022 to the 30th of June 2023**. There were 22 items in the survey, which were developed by the WP4 project team on the basis of a literature review and studies that applied similar research methods. In the process of data cleaning, we excluded the following cases: those without a valid country, cases with less than 50% of all questions answered, and cases with a response time of less than 166 seconds.

The final dataset contains **740 participants**, its structure is illustrated in Figure 1. No personally identifiable information was collected in the survey, so that the survey data was fully anonymous.

Survey data **cleaning and analysis was done with the programming language 'R'** on the basis of a csv file exported from our web survey tool. The raw data were securely stored at Fraunhofer ISI. The data, together with a list of survey variables, labels and values, was later shared within the project consortium via IMPULSE SharePoint for further analysis with the other work packages. The researchers will continue to use the data for publications. All data will be **deleted by January 2029** at the latest.

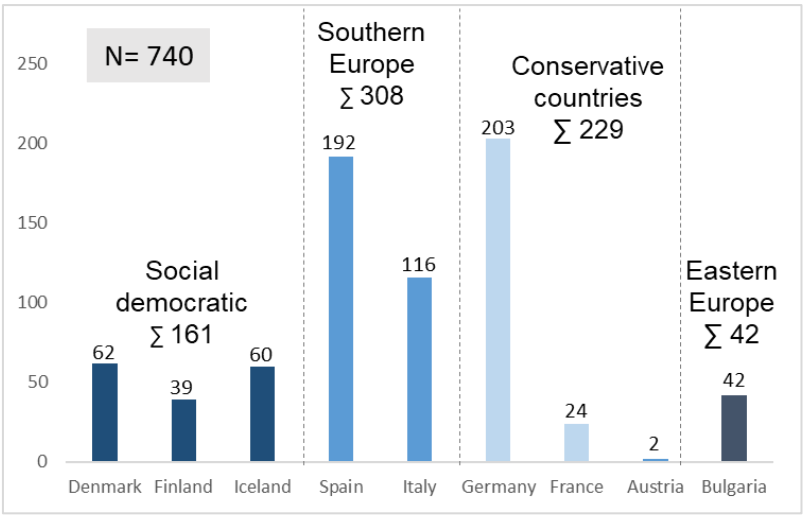

Figure 1 IMPULSE final data set

Our aim was to distribute the questionnaire to a wide range of people. However, there were some patterns and potential biases in the final data set that we carefully considered in our interpretation of the data.

- The majority of those surveyed (79%) have either graduated from or are currently studying at University.
- There is also an uneven distribution of age among respondents. The average age across the countries ranges from 38 years old in Spain to 48 years old in Germany.
- In addition, when we look at the income of the household, we see that about half of the respondents (53%) are in the 5th income quintile for their country.
- Although respondents reported high levels of digital skills overall, the results vary by country.[4] On average, respondents from Bulgaria had the lowest level of digital skills with a score of 70 out of 100, while respondents from Spain had the highest level with a score of 87.7 out of 100.

[4] To measure respondents' digital skills, the Digital Skill Index combines seven different items. They are derived from four different studies. All of them developed their items based on the Digital Competence Framework for Citizens (DigComp). The EU DigComp framework was developed by the Joint Research Centre of the European Commission. It measures digital skills in five areas of competence: Information and Data Literacy, Communicating and Collaborating,

3.2 Variables

On the basis of our data, we have indirectly measured the extent of DI or Digital Exclusion (DE). To do this, we used two **dependent variables** which are a) number of Online Public Services (OPS) used per year and b) whether the respondents have used eGovernment services (yes/no).[5]

In our analyses, we then made use of a number of **explanatory variables**. These included all sociodemographic variables included in the study: age, gender, income, education, etc. In addition, on the individual level, we also used the following explanatory variables: technology affinity and digital skills.[6]

To assess how cultures and institutions affect DI, we constructed **welfare regimes** as a set of additional explanatory variables. For this purpose, we grouped together those countries that, according to theory, belong to a particular regime type, such as social democratic countries, southern European countries, conservative countries or eastern European countries. However, this led to the possible inaccuracies listed below".

- It is possible for the data to be biased if countries, taken together, produce significant results that are not individually significant on their own.
- It is also possible that the country groups mask the effect of the other country which could be the opposite. This could be due to the dominant number of cases in one country.
- Interpreting the results is complicated by the fact that we can only ever speak of a (weighted) 'average' of a group of countries.

Due to these possible inaccuracies of data interpretation, we have also broken down digital inclusion by **country** (see chapter 4.2.2).

3.3 Expert consultations

As part of WP4.1, we have also carried out a number of expert consultations. Our main aim was to gain more qualitative evidence regarding why the patterns of DI/DE we identified in the survey data vary across European welfare states. In particular, we sought to answer the following research question: *How do the expert countries which belong to different welfare regimes deal with DI and the risk of digital exclusion for vulnerable social groups?*

In D4.1 (V1) we explained the objectives of these consultations and how we selected the interview partners. A total of **six experts** were consulted, covering the social democratic welfare regime, the conservative welfare regime and the southern European welfare regime.

Unfortunately, despite some significant attempts to involve more experts, we did not reach the expected number of experts (about 5 per welfare regime / 20 in total). It was also not possible to include experts from Eastern European welfare systems.

The experts were contacted on the basis of their expertise in relation to issues of digital inclusion, e-government or eID solutions. Interviews were conducted online and recorded and transcribed with the explicit consent of the interviewees for the sake of reliability.

Creating Digital Content, Security and Problem Solving. The items selected for the survey represent three of the five areas. They include digital skills needed to use eGovernment services as well as more general digital skills. The items were weighted between 1 and 4 as they cover different levels of complexity. Respondents were asked whether they had the competence on a Likert scale ranging from 1 — strongly disagree to 5 — strongly agree. These responses are multiplied by the respective weight and the result is the digital skills index. This results in the Digital Skills Index, which ranges from 20 to 100. Items are derived from Initiative D21 2021 and Digital Skills Monitor (TUM & Initiative D21, 2021, see also: Al Khateeb, 2017; Hatos et al. 2022)

[5] Unfortunately, we did not have the data to take into account the number of OPS that are actually available in each country.

[6] To measure respondents' digital skills, the Digital Literacy Index combines 7 different items. They are derived from four different studies. All of them developed their items based on the Digital Competence Framework for Citizens (DigComp). The EU DigComp framework was developed by the Joint Research Centre of the European Commission. It measures digital literacy in five areas of competence: Information and Data Literacy, Communicating and Collaborating, Creating Digital Content, Security and Problem Solving. The items selected for the survey represent three of the five areas. They include digital skills needed to use eGovernment services as well as more general digital skills. The items were weighted between 1 and 4 as they cover different levels of complexity. Respondents were asked whether they had the competence on a Likert scale ranging from 1 - strongly disagree to 5 - strongly agree. These responses are multiplied by the respective weight and the result is the digital skills index. This results in the Digital Skills Index, which ranges from 20 to 100.

The findings were used to critically contextualize what emerged from the survey data (see section 7) and are briefly summarized in the two tables below.

Barriers of DI...	Social Democratic	Southern Europe	Conservative
...on the political level	**Diminished significance of technical barriers** (reduced costs for digital devices, digital literacy improved, user-friendly interfaces)	Lack of a nation-wide **e-identity** useable in any region of the countries, such as Spain (here, there is such an eID, but barely used)	**Overburdening** of the citizens by centralizing access to services on smart phones (all ID documents, wallet), new risk such as losing it
...on the individual level	Increased **significance of non-technical barriers** (trust in services, government institutions, data management policies)	Lack of **technology affinity** might be a barrier, but also lack of trust in the institutions of the state	**Lack of trust** in government institutions that provide public services (less the lack of digital skills)
...on the technical level	However, limited **physical infrastructure** to access public services (e.g., due to geography of the country)	Services are **too complicated** (e.g., majority often fails to fill out forms)	**Functional illiteracy** (quickly understand access to public services also for foreigners)

Table 2 Summary of expert consultation: barriers of DI

Drivers of DI...	Social Democratic	Southern Europe	Conservative
...on the political level	Policy of "**Digitalization by default**" (norm: everyone shall participate, incl. opt-out-option, but steep walls for being integrated) **Long tradition of eID** / Central Person Index (CPI) (CPI numbers for each citizen, gov. information system), incl. learnings of failure, e.g. e-signature	Inclusive digital policies are based on **the digital needs of users** (this might imply to choose convenience over security requirements)	**Problem-oriented digital policy** (which asks first and foremost for the problem at hand, then for the technical solution that might fit) Digital policies are **oriented towards social rights**, e.g. participation, freedom of information, freedom of choice of services, privacy, tc.
...on the organizational level	**Public-private-partnerships**: integrate companies into service development (services providers, infrastructure owner/operator) Targeted **information campaigns** (for social groups, e.g. local outlets for elderly)	**Institutional embedding** of support for services, e.g. at high schools, in communities of target people in rural areas **Personal assistance** by service providers for vulnerable groups **Peer-to-peer training groups** (e.g. support to seniors by seniors, same language, perception of difficulties etc.)	**Institutional embedding of support** for digital service for vulnerable groups, e.g., providing contact points for the homeless **Empowerment of women** (due to their social role of supporters, e.g., if kids lack the skills and resources to access digital world)
...on the technical level	**Direct coupling** of national eIDs with both private and	Public services should be as **easy-to-use** like well-established commercial ones	**Functional literacy** (easy-to-understand public services, multi-language etc.)

	public services (e.g., banking) **Incentives / benefits** for the usage of OPS, e.g. enrolment for universities only online	

Table 3 Summary of expert consultation: drivers of DI

4 Findings: Social and cultural factors

In this section we examine the social and cultural factors of the acceptance of eID solutions. For this purpose, we first show the level of DI in Europe based on our data (*section 4.1*). We will then take a look at the social factors (*section 4.2*) and the cultural factors (*section 4.3*).

4.1 Level of DI in Europe

We have used two dependent variables to measure the level of DI. Firstly, the **number of OPS which respondents use per year** and secondly, **if the respondents have already used eGovernment services** at all. As respondents could only answer yes or no, the latter question is a rather weak indicator of DI which is why we have used this variable only to gain some additional evidences.

With regard to the frequency of using OPS, our data show that, on average across all countries, respondents use **5.3 services per year**. By comparison, private services are used almost two times more, averaging ca. 12 per year. As Figure 2 shows citizens in Germany (mean: 2.5) and Bulgaria (3.3) are most at risk of being digitally excluded from OPS. Whereas citizens in France (7.7), Finland (6.7), Spain (6.2) and Denmark (5.9) are less affected. Iceland (5.3) and Italy (4.8) occupy a medium position.

Looking at our theoretical assumptions, Germany is surprisingly low in digital inclusion, while France is surprisingly high in becoming digitally included. We were also surprised by the high level of digital inclusion in the countries of southern Europe. Less surprising is the high propensity of the Scandinavian countries and the low propensity of Bulgaria, representing the Eastern European countries.

Quite a similar pattern of DI occurs if we look at the usage of of e-government services. While for the large majority of countries, **nearly every citizen has already used e-government services**, only people from Bulgaria, but also (and this is in contrast to our assumption) also Germany are at risk of DE when it comes to using such services. This is illustrated in Figure 3.[7][8]

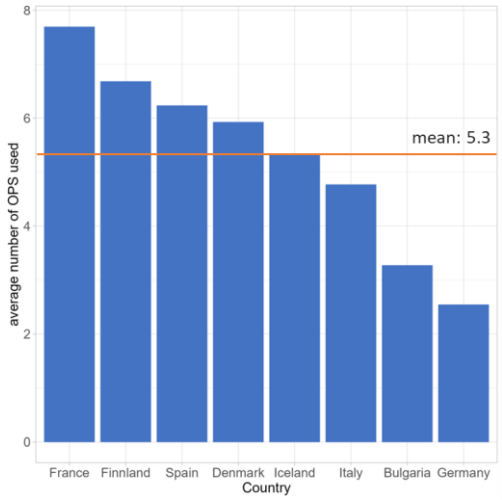

Figure 2 Number of OPS used per year

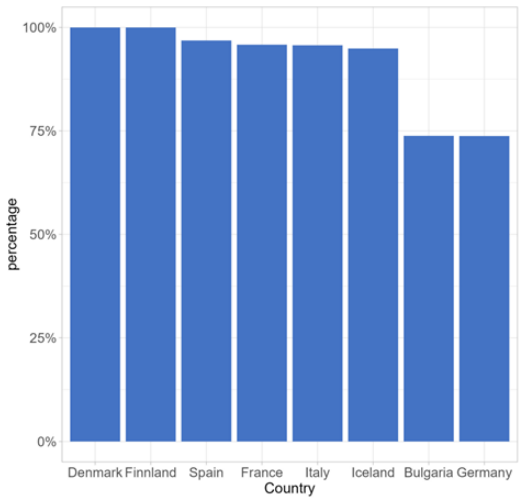

Figure 3 eGovernment services used at all (yes/no)

Our findings for Germany are consistent with other studies, which show that most administrative services are received in analogue form, with only a few services mostly used online (TUM & Initiative D21 (2021).

[7] However, we did have a small number of 'no' answers to this question. It is possible that this question is a weak indicator of digital inclusion. This is because 'yes' means that only one service had to be used. For example, in some countries tax filing is already mandatory.

[8] Again, unfortunately, we did not have the data to analyse these results with regard to the number of OPS that are actually available in each country.

With this first impression of DI in Europe in mind, we now have a look at the social and cultural factors that might explain the observed differences.

4.2 Social factors

The social factors cover sociodemographic variables, but also attitudes such as technology affinity and digital skills (cf. Addo/Senyo, 2021). In a first step, we only included **socio-demographic variables** such as age, gender, education or income into a regression. Unfortunately, according to this model, barely any factor appeared to be strongly significant. Only post-secondary education appeared as a weakly significant factor meaning that people with higher education seem to use OPS more often than lower educated respondents (see Annex A.1, model 1).[9]

Surprisingly, in the first three models, age did not emerge as a significant factor. However, in the fourth model **age** re-emerge as a factor in which we included the welfare regimes. This may support our findings in our literature review that age may only matter in some countries, such as Germany, but much lesser in others (Jackwerth-Rice et al., 2023).

The slightly significant association between **DI and age** is shown in Figure 4. For all respondents, there is a slight increase in the number of services used per year up to the age of 40, and a decrease from the mid-50s onwards. Overall, the curve remains flat indicating the weak association of DI with age.

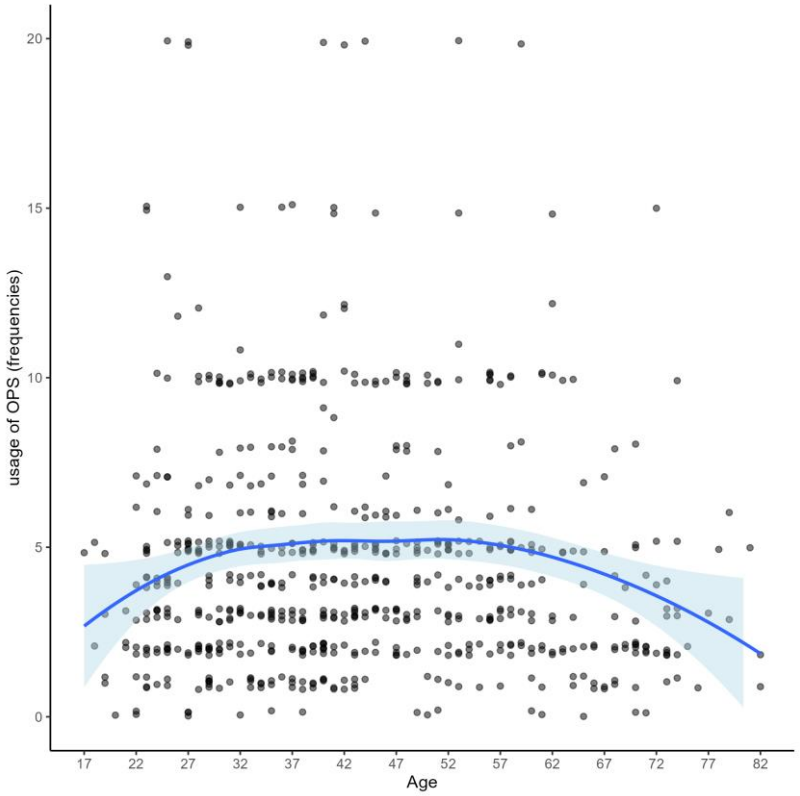

Figure 4 Impact of age on the number of OPS[10]

It appeared more significant, that **digital skills** (**technology affinity**) are important factors of DE (see Annex A.1, model 2 and 3). Figure 5 clearly shows that OPS are used more often if the level of digital skills increases (digital skill index, see section 3.1.2 'Independent variables').

[9] The other socio-demographic characteristics such as gender, household income, ethnicity, nationality or place of residence were not found to be statistically significant in this model.

[10] The graphs in figure 4, 5, 6 were created using the R package ggplot2 (Wickham 2016).

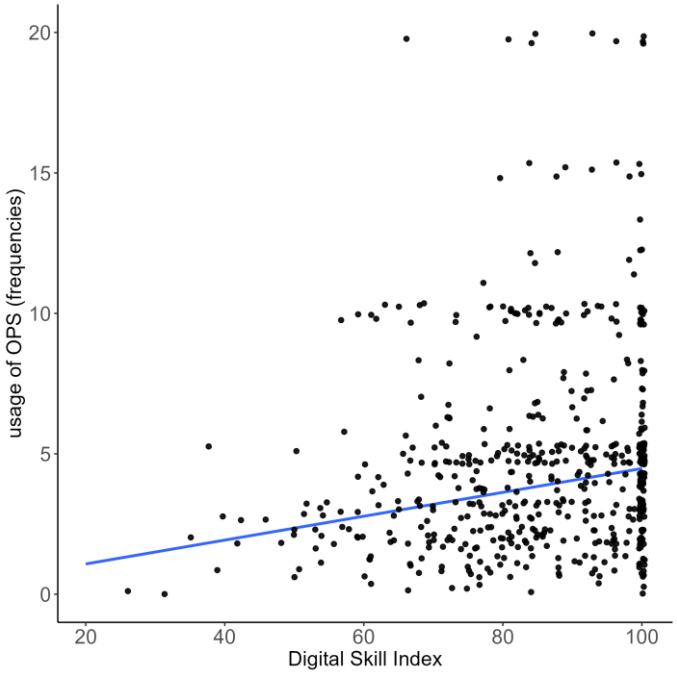

Figure 5 Impact of digital skills on the frequency of OPS

Similarly, we can see that people who have used e-governance services have a higher level of digital skills then those who have not yet used such services at all. This is illustrated in Figure 6.

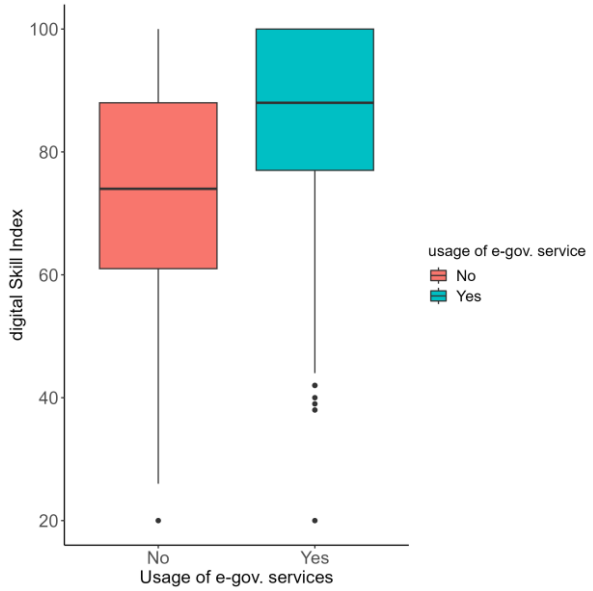

Figure 6 Digital skills and usage of eGovernment services

All in all, it is mainly **digital skills** and **technology affinity** who appear to be social factors for DE. Digitally skilled people are then those who are able to use search engines, office applications, find relevant information on the Internet or store data (see Annex A.7 / Digital Skill Index). Promoting DI would then mean supporting people who are less digitally skilled or less technologically affine. How this could happen, is discussed in more detail in section 7 of this report.

So far, these results appear to be in line with those of other studies. Accordingly, socio-economic or socio-demographic characteristics such as age (Alexopoulou et al., 2022), but also individual abilities such as attitudes, skills and trust, explain why people do not use government online services (Robles et al., 2021; see also Jackwerth-Rice et al., 2023). However, as Robles et al. (2021) point out, the individual ability to use digital solutions is often closely related to socio-economic characteristics, e.g. the lower the income and education level, the lower the digital skills; the younger the user, the more likely they are to have a high level

of digital skills. This suggests that social policies could be particularly effective in digitally integrating those people who lack the education, income or the knowledge of how to use eID solutions and OPS.

Our results show that high age, low digital skills, lower secondary education and low affinity with new technologies are the key social factors for digital exclusion.

Based on these results, it is possible to identify social factors that influence the likelihood that people accept new eID solutions and are thus more at risk of being digitally excluded. However, we underline the first three social factors because technology affinity seems to be strongly related with digital skills.

- Age
- Digital skills
- Education
- (Technology affinity)

It is interesting to note, however, that the importance of digital skills is reduced when welfare states are taken into account (see Annex A.1 / model 4). This might be due to cultural factors which we discuss in the next section.

4.3 Cultural factors

The cultural factors explaining why the level of DI differs across Europe are discussed in the next section. After that we assess the cultural factors with regard to the countries involved in our survey. We did this due to the statistical inaccuracies explained in section 3.2.

4.3.1 Welfare regime

Based on our theoretical framework (see section 2), we expected citizens from southern and eastern European countries to be most at risk of DE. Conversely, we expected social democratic countries to have the highest levels of digital inclusion and conservative countries a medium level.

To verify our assumption, we introduced all four types of welfare regimes as variables in our regression models, in which the conservative welfare regime was used as the reference regime (see Annex A.1 / model 4). Our expectations were partly confirmed by our results.

The model shows that citizens from the **social democratic countries included in the survey are the least at risk** of digital exclusion. This is also the case when their digital skills are low, as shown in Figure 7. This analysis provide further evidence that digital skills are an important socio-political factor of digital inclusion.

Contrary to our expectations, however, **individuals from Spain** which belong to the southern European countries are also **barely at risk of being digitally excluded**.

People from Eastern Europe may also be less exposed to the risk of digital exclusion than expected because according to our data they are more digitally included than people from conservative countries. However, this result is not significant, which might be due to the limited number of cases (see Figure 1, p. 12)

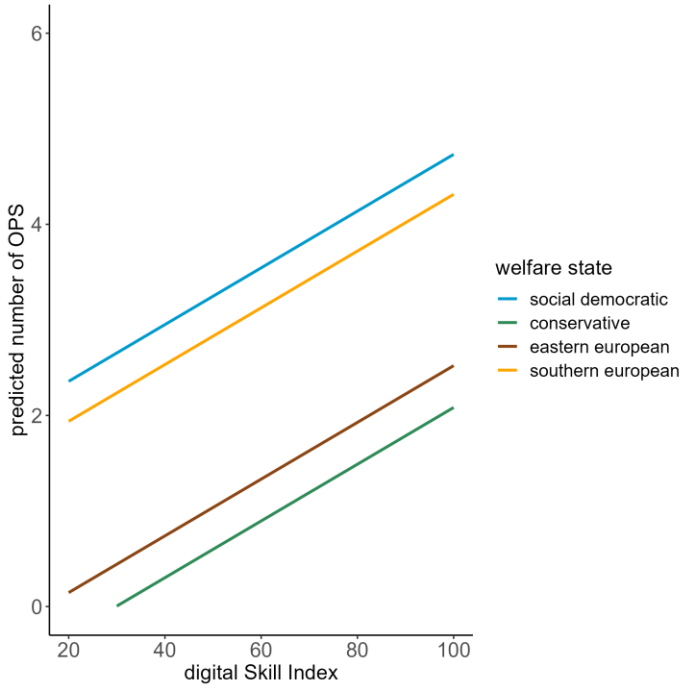

Figure 7 Impact of digital skills on the usage of OPS in all welfare states[11]

Another factor we have discussed above was age. Our analysis have shown, once we introduce the welfare regimes, **age** emerged as significant factor for DI when it comes to the number of OPS. However, this is at a low level of statistical significance. Moreover, as Figure 8 shows, with rising age until approximately 70 years, the usage of OPS increases and then decreases slightly. Thus, we consider age as a factor of DI, however its **significance appears to be weak**.

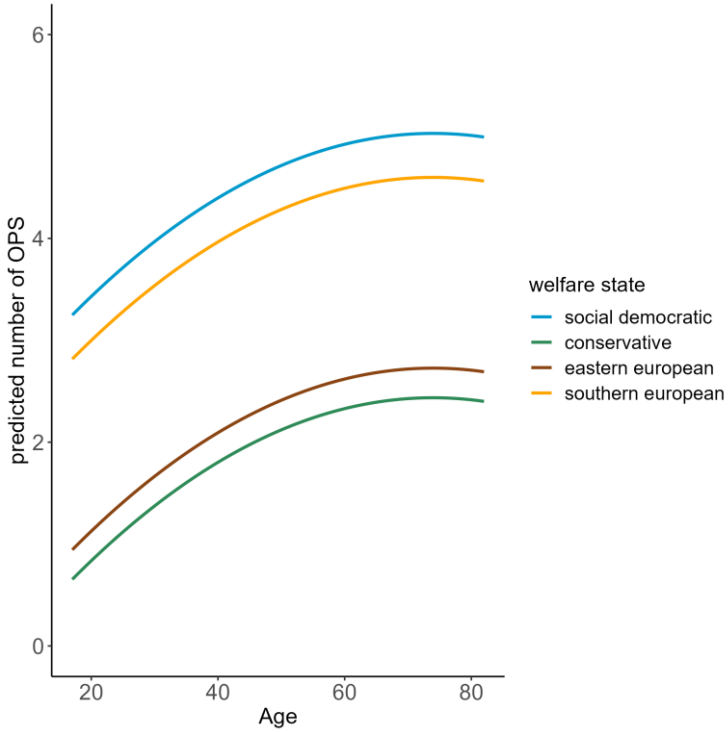

Figure 8 Impact of age on the number of OPS in all welfare states

Also, in model 4, which include the welfare states as variables, the **lack of digital skills** seems to have a less significant factor of digital exclusion. The patterns observed here are confirmed when we look at the usage of e-government services as a measure of digital inclusion (see Annex A.2). The data from model 3 shows here,

[11] Figure 7 and 8 were created using the R package ggeffects (Lüdecke 2018).

firstly, that although not significant in the case of Eastern Europe, **people from conservative and Eastern European regimes are more digitally excluded**. *Second*, these data confirm that social democratic countries and countries in southern Europe are at the lowest risk of digital inclusion, regardless of the digital skills of their citizens.

From a welfare state perspective, the policies and institutions of conservative countries like Germany or Eastern European countries like Bulgaria seem less effective in reducing the risk of digital exclusion for their citizens.

All in all, this leads us to further interim results. Unfortunately, we have not found any clear factor that is similarly significant across all four welfare regimes. Instead, we found evidence of social and cultural factors that are specific to welfare regime, as shown in Figure 9.

- digital skills (for Eastern Europe)
- technology affinity (for conservative countries)
- age, education (Southern Europe)
- no significant factors for Scandinavia

	Dependent variable:			
	Number of OPS used			
	eastern european	conservative	social democratic	southern european
	(1)	(2)	(3)	(4)
Age	0.01	0.03	0.02	0.05*
GenderMale	-0.39	-0.41	0.41	-0.64
EducationVocational	-1.09	0.64	2.05	0.78
EducationUniversity	-0.29	0.45	1.85	1.91*
Income1	0.32	-0.80	-0.79	-1.86
Income2	-0.06	-2.03	0.14	-0.65
Income4	1.51	0.36	-1.09	0.90
Income5	0.12	-0.79	-0.02	1.13
ÉthnicityMinority	0.07	1.64	-1.07	-0.51
CitySmall	-0.87	0.18	-0.69	0.15
CityMajor	-0.99	1.16	-0.80	0.75
CitizenshipResident	1.65	-0.67	-0.78	0.85
new Technology	-0.28	0.69*	-0.04	0.12
digitalSkillIndex	0.07**	0.03	0.04	0.04
Constant	-0.29	-3.13	1.21	-2.43
Observations	27	172	123	239
R^2	0.70	0.09	0.07	0.07
Adjusted R^2	0.34	0.005	-0.06	0.01
Residual Std. Error	1.42 (df = 12)	4.14 (df = 157)	3.85 (df = 108)	3.74 (df = 224)
F Statistic	1.96 (df = 14; 12)	1.06 (df = 14; 157)	0.54 (df = 14; 108)	1.23 (df = 14; 224)
Note:				*p<0.1; **p<0.05; ***p<0.01

Strongly significant | Weakly significant

Figure 9 Regime-specific factors of digital inclusion[12]

However, even factors such as digital skills, which we found to be highly significant in section 4.2, show a smaller impact on DI if we consider the institutional context. This may be an indication of the importance of policies and institutions for reducing the risk of digital exclusion.

[12] The regression output, as well as all following regression outputs were created using the R package stargazer (Hlavac 2022).

Our results indicate that in the conservative and eastern European welfare states people are more likely to be at risk of DE than in any other cultures. However, it appears that the Nordic and Southern European welfare states are more effective in promoting DI.

4.3.2 Countries

	Dependent variable:
	Number of OPS used
Age	0.05***
GenderMale	-0.22
EducationVocational	0.86
EducationUniversity	1.06*
Income1	-0.02
Income2	-0.28
Income4	0.08
Income5	-0.06
EthnicityMinority	-0.55
CitySmall	0.15
CityMajor	0.97**
CitizenshipResident	0.13
Denmark	2.62***
Finnland	3.12***
France	5.42***
Germany	-0.97
Iceland	1.24
Italy	0.76
Spain	2.75***
new Technology	0.32*
digitalSkillIndex	0.03**
Constant	-3.34**
Observations	561
R^2	0.23
Adjusted R^2	0.20
Residual Std. Error	3.57 (df = 539)
F Statistic	7.57*** (df = 21; 539)
Note:	*p<0.1;* ***p<0.05;*** p<0.01

Figure 10 Factors of DI incl. countries

The previous chapter identified social and cultural factors that influence the acceptance and adoption of eID solutions in different welfare regimes. Due to our statistical challenge of interpreting groupings of countries into welfare regimes (see *Section 3.2*), in this section we look at the country-level of DI.

When countries are introduced into our models, **age** reappears as a highly significant factor with seniors using OPS more often, as shown in Figure 10 (cf. Ciesielska et al., 2022). The risk of DI also seems to be reduced by living in a **major city** or having a **post-secondary education**. However, the latter factor is only weakly significant.

Interestingly, in this model, compared to the other models discussed above (with or without the inclusion of welfare systems), **digital skills** and **technology affinity** seem to explain the variation in DI less clearly.

If we look at the impact of the countries on DI, the results are as follows: Being citizens of **Denmark or Finland** significantly decreases the risk of DE in comparison with Bulgaria.[13] This suggests that these countries with social democratic welfare systems are more effective at promoting DI.

This means, with Iceland not significant, this model partly confirms that the Nordic countries seem to better tackle the issue of DE than eastern European countries. Thus, contrary to the social democratic welfare regimes, Bulgaria seems to be less effective in promoting DI.

For the other welfare regimes the interpretation of the results is more ambiguous. This means, being a **French** citizen clearly increases DI compared with Bulgarians, whereas being **German** does not. A similar picture emerges for the European welfare regime with only being **Spanish** citizen appears to increase the usage of OPS. **Italy** shows no significant effect.

Our findings do not point to clear-cut social or cultural factors across cultures. What we have found, however, is that some social groups — seniors, less digitally skilled, lower educated — may be more at risk of DE than others. We have also found clear evidence of institutional contexts in which the risk of digital exclusion is addressed in different ways (e.g. quite effectively in Denmark and Finland).

Our results for countries are summarized in Table 4. Here, a country-specific factor is considered important if it appears to be relevant across welfare regimes (rows) or within welfare regimes (columns). This means, if two countries are placed in the same cell, we took this as an indication of the importance of a factor. However, if we proceed in this way, we only come to two conclusions.

- **age** remains an important factor (although the overall significance is weak and the results remain ambiguous)[14]
- **secondary education** positively impacts on DI[15]
- **digital skills** are an important driver of DI

For the other factors, we found insufficient significant results to draw meaningful conclusions.

[13] Bulgaria is used as a reference country for the others.
[14] Age is negatively correlated in Denmark, and positive in Finland, Spain, Italy and Germany.
[15] However, this contrasts with some of our findings shown above, which highlighted post-secondary education as a more significant factor.

Socio-political factors	Social democratic countries	Conservative countries	Southern European countries	Eastern European countries
Age	Denmark*[16], Finland*	Germany*	Spain***, Italy*	
Gender	Denmark*			
Income 1[17]	Denmark**			
Income 4	Denmark***			
Secondary school			Italy**	
Post-secondary education				
Town			Italy**	
City			Italy**	
Technology affinity	Denmark**			
Digital skills	Denmark*			Bulgaria**
Level of statistical significance: *** high; ** medium; * low				

Table 4 Country-specific factors of digital inclusion

[16] For age in Denmark, we found a negative correlation.
[17] In the survey, there were country-specific quintiles of income per year, with categories ranging from 1 to 5.

5 IMPULSE' contribution to DI

Based on the social and cultural factors of DI outlined above, we point out that seniors, less digitally skilled and lower educated people are those social groups that are most at risk of being digitally excluded. This section asks if a technical solution such as IMPULSE could be a driver of DI.

Therefore, for each social group, we now assess how IMPULSE could support them for using OPS more often.[18] In order to do this, we are going to take a closer look at the digital needs of these social groups and assess the extent to which IMPULSE is suitable for encouraging them to use OPS more often.

5.1 General perception of IMPULSE

Before looking at how social groups perceive IMPULSE, we look more generally at how IMPULSE was rated by all respondents as a possible eID management solution. In fact, **IMPULSE was perceived as a fairly positive solution by virtually all of the respondents**.[19]

Approximately 77% appear to be open if IMPULSE would be established as eID solution, as shown in Figure 11. Moreover, over half of the participants would use IMPULSE instead of an alternative such as a digital version of one's identity card. This is illustrated in Figure 12**¡Error! No se encuentra el origen de la referencia.**.

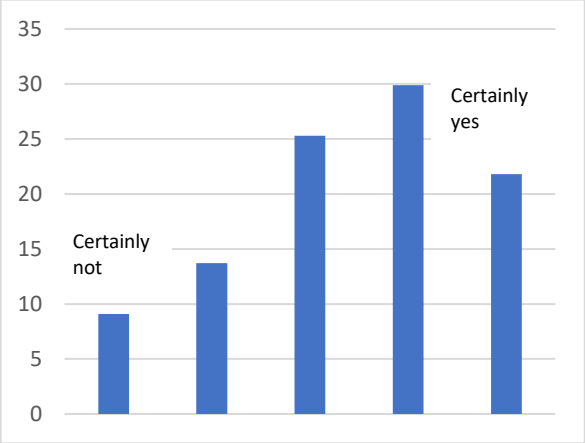

Figure 11 Usage of IMPULSE as an eID tool

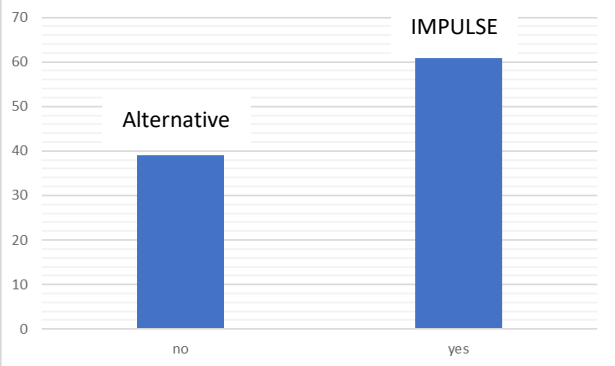

Figure 12 IMPULSE or alternative

Also across all welfare regimes IMPULSE is seen as a fairly good solution. A clear majority would use IMPULSE and not even one quarter would rather reject any usage.

WR	1 (not at all)	2	3	4	5 (certainly yes)
Social Democratic	25 (15.5%)	31 (19.3%)	42 (26.1%)	41 (25.5%)	22 (13.7%)
Conservative	23 (10.2%)	39 (17.3%)	69 (30.5%)	61 (27.0%)	34 (15.0%)
Eastern European	1 (2.4%)	1 (2.4%)	5 (11.9%)	11 (26.2%)	24 (57.1%)
Southern European	18 (5.8%)	30 (9.7%)	71 (23.1%)	108 (35.1%)	81 (26.3%)
Total	67 (9.1%)	101 (13.7%)	187 (25.4%)	221 (30.0%)	161 (21.8%)

Figure 13 Assessment of IMPULSE across welfare regimes[20]

[18] To analyze specific sociodemographic groups is in line with research literature (Pérez-Amaral et al., 2021).
[19] Participants were asked: "*Would you use IMPULSE instead of the digital identity (log-in) systems you currently use (like username/password, smartcard, PIN, etc.), if IMPULSE were available?*"
[20] The table was created using the R packages flextable (Gohel & Skintzos 2023) and janitor (Firke, 2023).

5.2 Perception vulnerable social groups

We now assess if IMPULSE could be a driver of DI. For this purpose, we look more closely at the social perception of the IMPULSE solution as well as digital needs of the social groups identified being at risk of DE, based on the social and cultural factors. In fact, for each social group we assessed their digital needs with regard to the following issues (see also Annex A.7)

- **Perception** of IMPULSE as suitable solution (*survey question: Would you use IMPULSE instead of the digital identity (log-in) systems you currently use?)*
- Personal requirements to have **control** over personal data: (*survey question: For many people, it is very important to have "control over their data". Having "control over your data" has many dimensions. Below is a list of some dimensions. Please indicate the three most important in your opinion.)*
- **Preferred log-ins** for online services (*survey question: Please indicate below which three digital identity (log-in) technologies you prefer to use for your log-ins*.)
- Suggestions for **improving** OPS (*survey question: Thinking about your experience with eGovernment, what aspects should be improved the most? Please indicate what you consider to be the three most important improvements*)

5.2.1 Senior citizens

In our study, the seniors are all people that are 60 years or older. It is interesting to note that seniors have a similarly positive perception of IMPULSE as younger citizens who are here all respondents that are 59 year or younger. As Figure 14 a large majority of seniors would use IMPULSE or at least seems to not reject the solution.

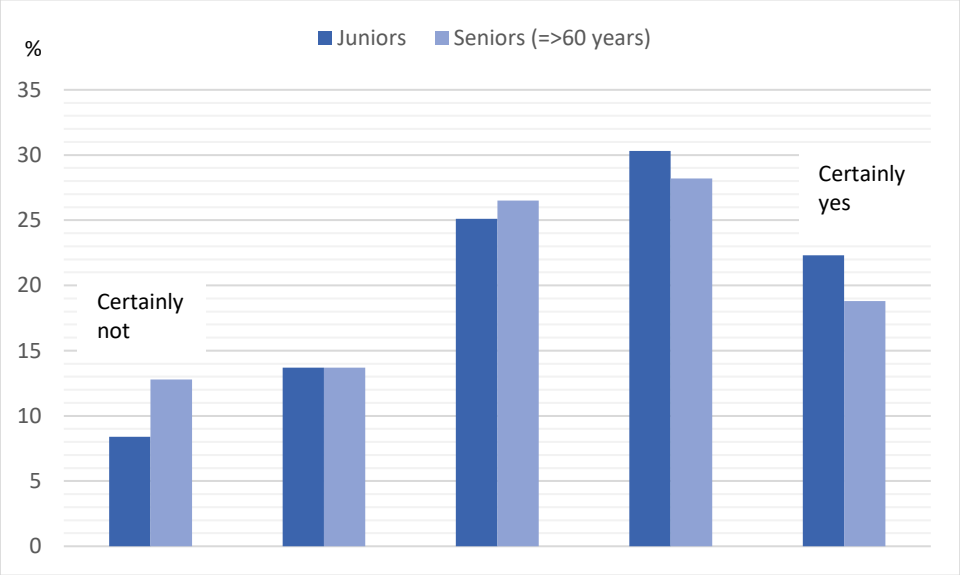

Figure 14 Seniors' perception

Also, for both seniors and juniors alike, the control of data is important. As Figure 15 shows, it is particularly more important for seniors that OPS do **not use more data than available** for the services. Also, the services should await the **consent of the users** before they use personal data. In addition, services shall **delete personal data** if they are requested to do so. For seniors it appears particularly important that online service provider do **not refuse their service** if user reject the usage of its personal data for advertisement.

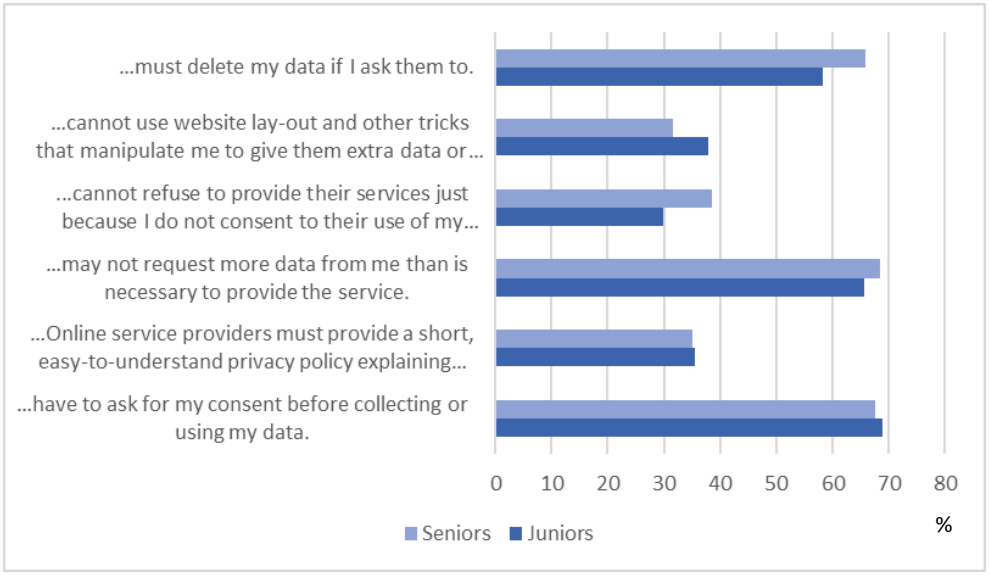

Figure 15 Seniors' control of data

For seniors and juniors, **user name and password** is the most preferred log-in solution. In fact, as Figure 16 shows, nearly 80% of the seniors would prefer using user name and password and over 40% of them **PIN/TAN** options. In comparison with juniors it is interesting to note that senior citizens report using less of the biometric log in options like face and fingerprint recognition.

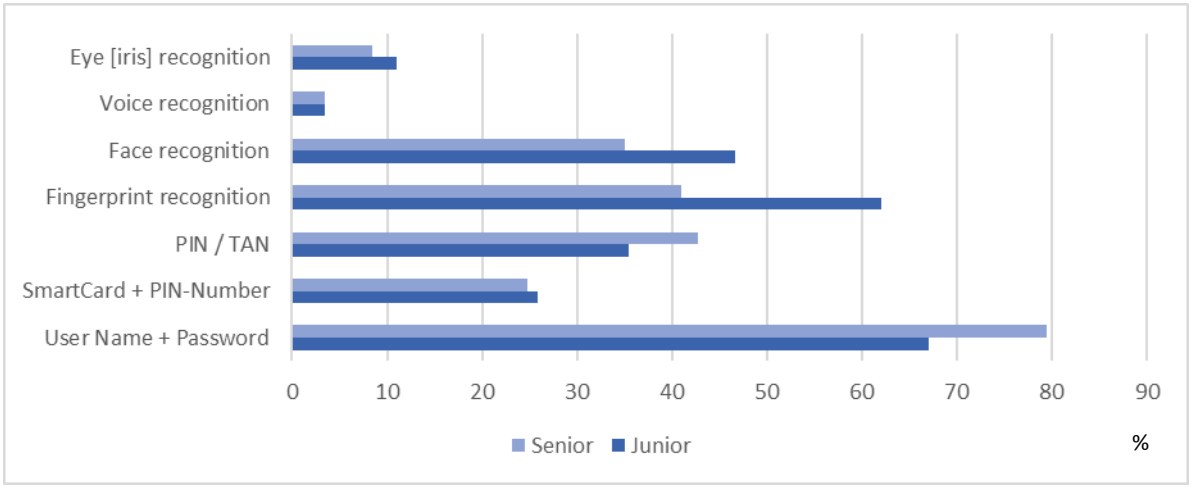

Figure 16 Seniors' preferred log-ins

Seniors and younger people make similar suggestions for the improvement of eGovernment. As Figure 17 shows, for seniors (and younger people) it would be most important to simply have **more OPS available** and to ensure that all eGovernment services could be completed online. Also, such services should be **easy and fast to use**.

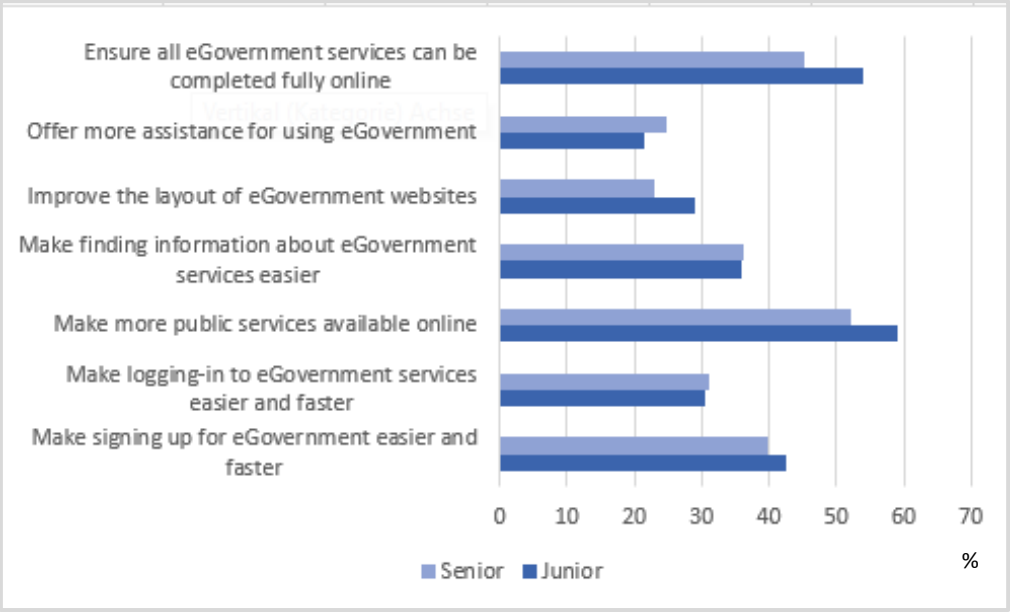

Figure 17 Seniors' suggestions for improvement

IMPULSE is unlikely to encourage elderly people to use OPS more often. Although this social group appears to be very receptive to IMPULSE, their digital needs for controlling data, preferred logins or improved services could also be met by other eID solutions. Indeed, also non-technical measures, such as making OPS more available or provide more information about them may be more effective.

5.2.2 Less digitally skilled

In our study, according to the digital skill index, the digitally less skilled are all those who are able to use search engines, office tools or save files on their devices. This is the case for all individuals who are classified as belonging to the level 1 or 2 of digital skills (see Table 5). Whereas the digitally skilled are those who use cloud applications or online services, re-install computer programs or are able to read basic computer code.

Weight¤	I know how to…¤
1¤	…use Google or other internet search engines¶ …use email or social media¶ …use Word or Powerpoint¤
2¤	…find relevant information and forms on websites of state agencies like ([*country-specific example, e.g. local government office, unemployment agency*])¶ …save or store files (documents, music, films etc.) on my device and retrieve them when I want them¤
3¤	…use Cloud Applications like Dropbox, iCloud, Google Drive, SharePoint to store and share documents¶ …use online services like e-banking, e-governments, e-hospitals etc.¶ …re-install or update computer programs¤
4¤	…read a simple computer code and make basic changes to it¤

Table 5 Levels of digital skills

Regarding the overall assessment of IMPULSE, our results show that the less digitally skilled seem less enthusiastic than the highly skilled. However, they are **generally open or neutral towards the IMPULSE** solution. However, more of this group are not at all convinced by IMPULSE. This is illustrated in Figure 18

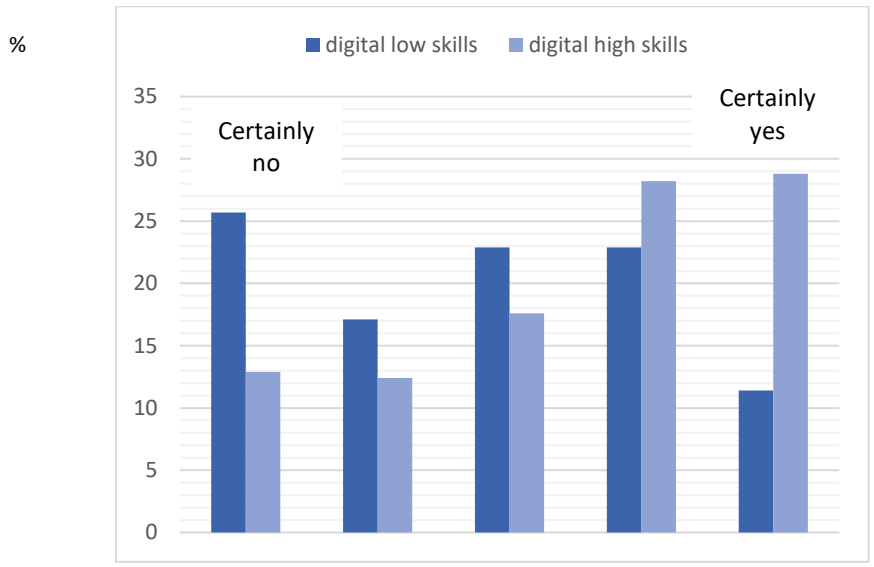

Figure 18 Less digitally skilled' perception

The **data control requirements** for the less digitally skilled are similar to those for the other group, albeit at a different level. For both groups, it is important that **service providers do not ask for more data** than is necessary for the less digitally skilled. This is a strong argument for a solution like IMPULSE that minimises the sharing of personal data with the service provider.

In addition, this group (similar to the more digitally skilled) considers it important that the service provider only **collects data with the individual's consent**. However, this is a requirement that is easily met by other eID solutions. Those with low digital skills also consider it important that **services delete their data** when requested, compared to those with higher digital skills. This requirement is also not specific to IMPULSE.

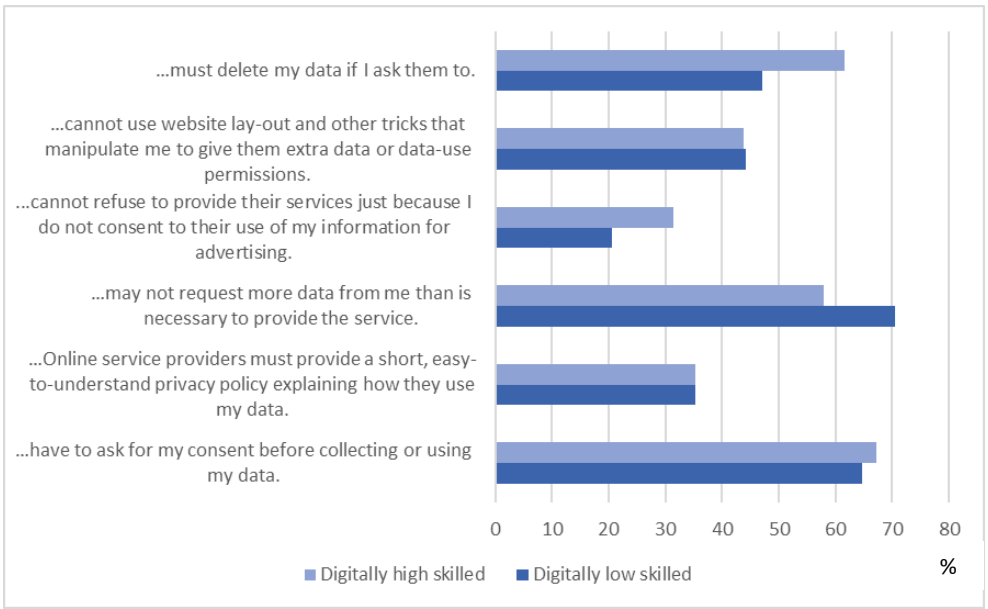

Figure 19 Less digitally skilled' control of data

Similar priorities emerge for both groups, albeit at a different level, when asked about preferred login methods, as Figure 20 shows. For around 75% of the low digital literate, **username and password is the preferred login** solution, followed by **fingerprint recognition**. An argument for IMPULSE could be that facial recognition is preferred by 40% of the low digitally literate to log in.

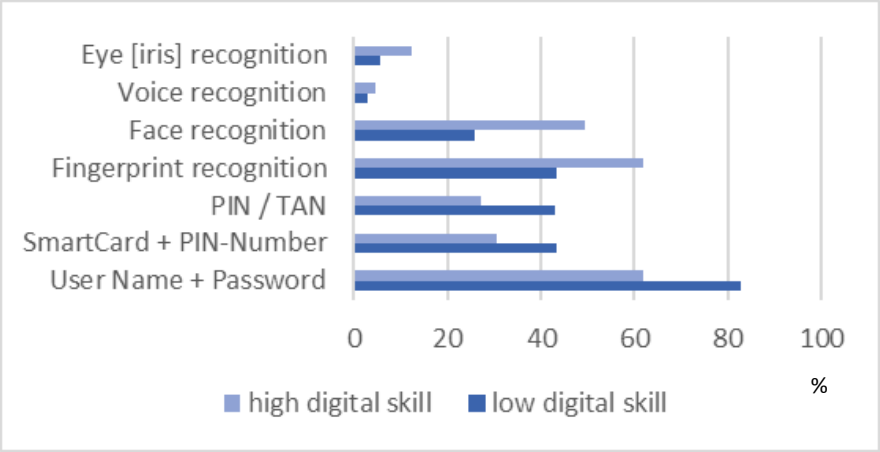

Figure 20 Less digitally skilled' preferred log-ins

When it comes to the suggestions for improving eGovernment we see quite large differences between people with higher and lower digital skills. As Figure 21 shows, while people with high digital skills show a need for a higher availability of eGovernment services, people with low digital skills emphasise their **need for assistance, more information as well as easy and fast to signing up** for such services.

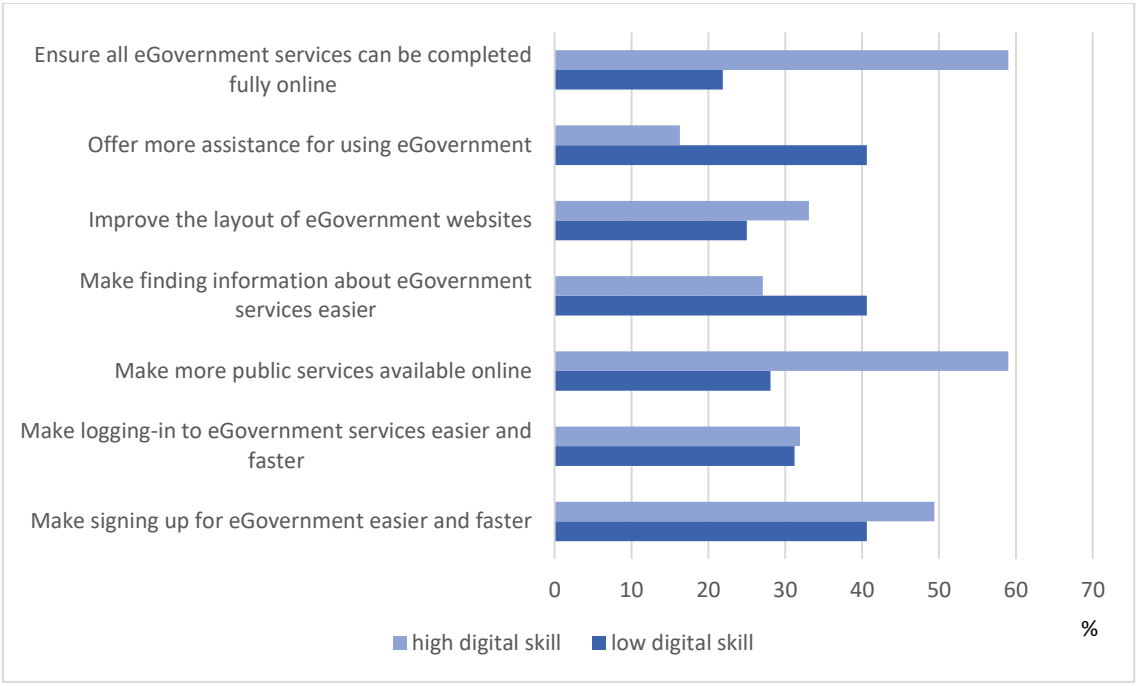

Figure 21 Less digitally skilled' suggestions for improvement

The less digitally skilled are quite open to IMPULSE. However, they are less euphoric than the more digitally skilled. For this group, IMPULSE could increase DI, if service providers use personal data in a restricted way. However, their other digital needs, such as personal consent to the use of personal data, but also their desire for more support, information and easy and fast enrolment, could also be met by other eID solutions.

5.2.3 Lower educated

Those with primary or secondary education are considered as having a low level of education. Those with upper secondary education, still in vocational training or studying at university are defined as having higher education.

According to our data, the respondents with lower education show a **higher interest in using IMPULSE** than people who are still involved or have completed a post-secondary education. Figure 22 also shows that ca.

70% of the lower educated respondents report that they would use IMPULSE compared to ca. 50% of the respondents with a higher education level.

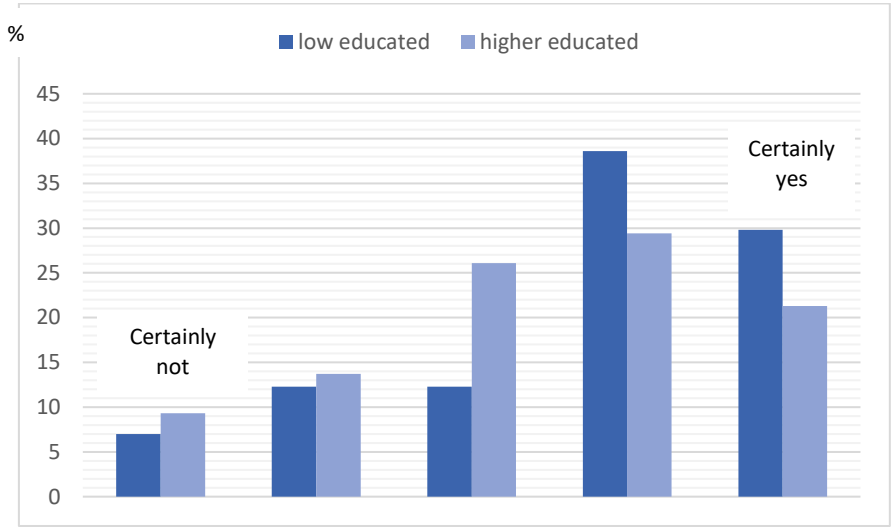

Figure 22 Lower educated' perception

Both groups responded similarly to the data control question. However, the lower educated responded at a slightly lower level. Figure 23 shows that, for both groups, it is most important that **services restrict the use** of their personal data and **delete it if the user wishes to do so**. The first requirement could be an argument in favor of IMPULSE, the second, however, can also be met through legal conditions.

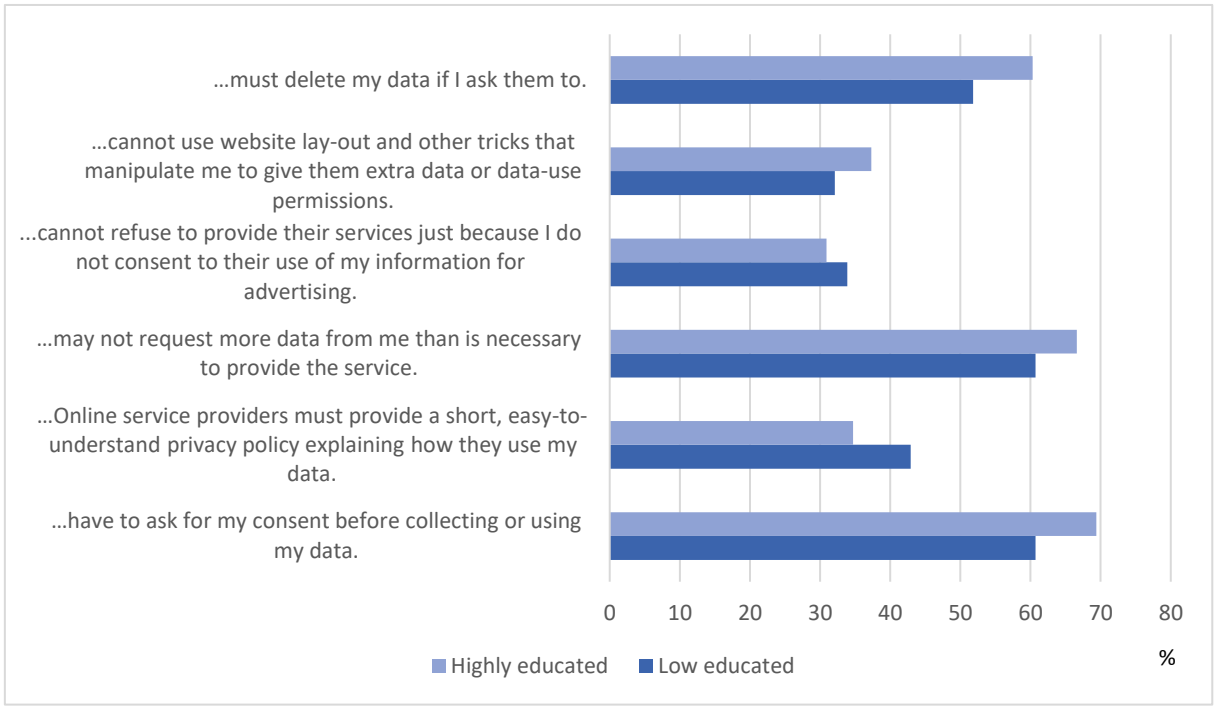

Figure 23 Lower educated' control of data

With regard to preferred log-ins, for lower educated people reported, using one's **user name and password** is the most preferred log-in solution. It is interesting here that, compared with better educated people and seniors, **fingerprint recognition** appear to be a preferred solution for log-ins. Both digital needs are hardly covered by IMPULSE.

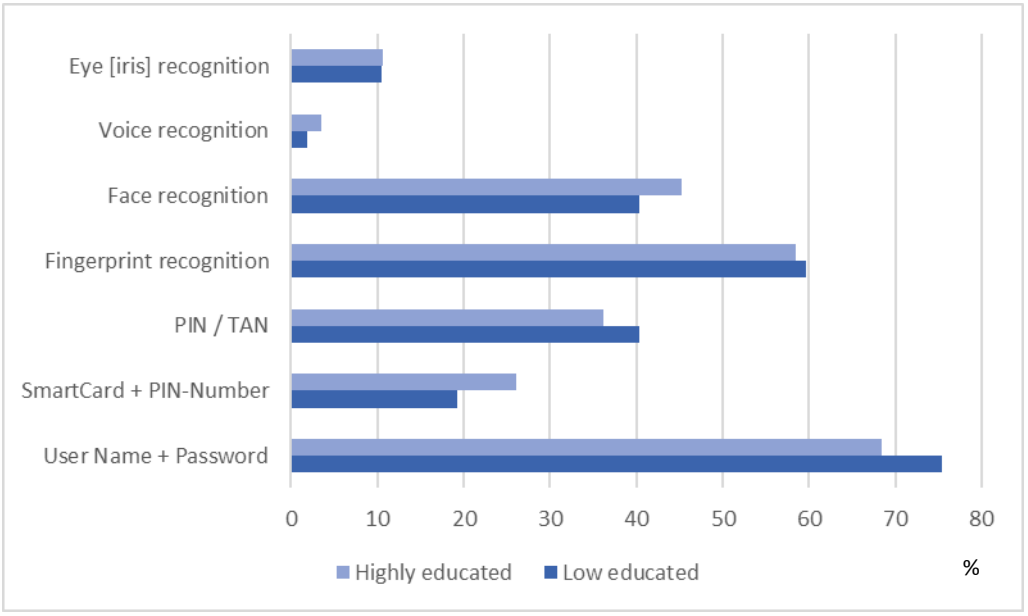

Figure 24 Lower educated' preferred log-ins

As Figure 25 demonstrates, the three most common suggestions from people with lower education are: making more public services **available** online, ensuring the **all eGovernment services can be completed fully online** and making **signing up for eGovernment** services easier and faster.

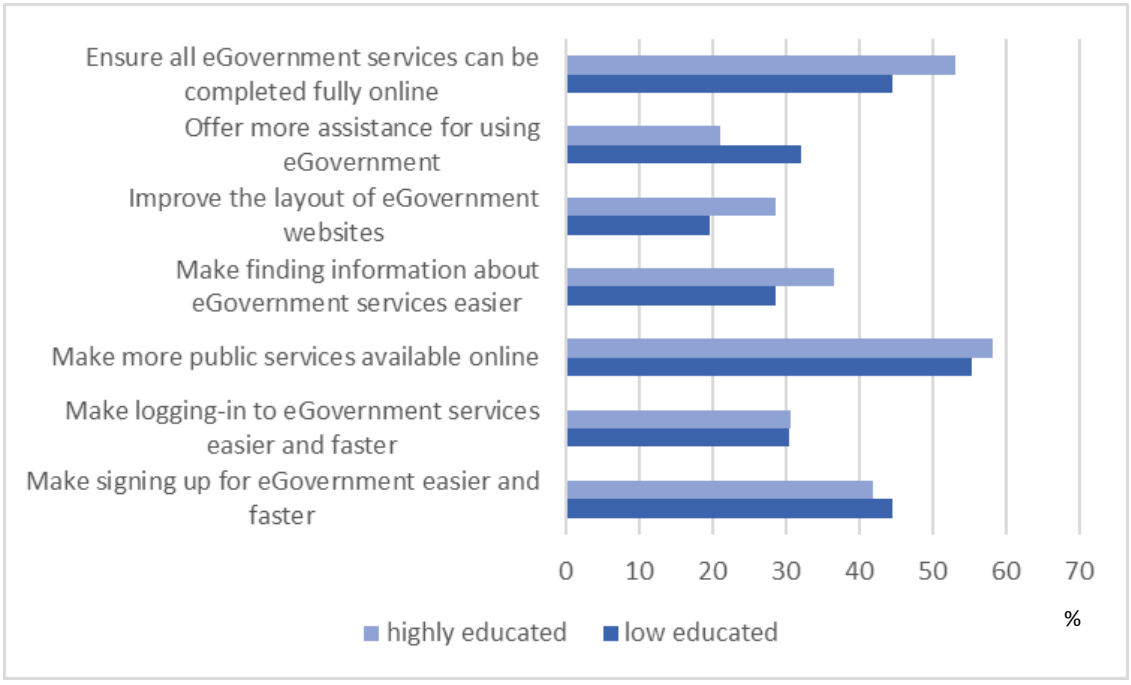

Figure 25 Lower educated' suggestions for improvement

Respondents with a lower level of education are more open to the idea of IMPULSE than those with a higher level of education. Similar to the less digitally skilled, the less educated may trust OPS more if the service provider restricts the use of personal data. This could be an argument in favour of IMPULSE. However, other digital needs like data deletion or login preferences are not IMPULSE-specific.

The digital needs of all social groups are summarized in the table in Figure 26. Based on these results, we conclude that **IMPULSE is unlikely to have a widespread impact on DI**. However, a key argument which

emerged across all social groups, is that IMPULSE makes service providers to limit how personal data gets used. The **restricted use of personal data by the service provider** appears to be a key argument across all social groups for using OPS more often.

	Openness for IMPULSE	Control of personal data	Preferred log-ins for OPS	Suggested improvements
Senior citizens	High (majority would use it)	Desire for restricted use of their data, deletion upon request	User name & password most preferred,[21] biometrics less	Higher availability of OPS, easy and fast to use
Less digitally skilled	Medium, but still majority seems to be open for it	(similar with seniors)	User name & password most preferred, then fingerprint recognition	More assistance and information, easy and fast signing up for OPS
Lower educated people	High, a clear majority would use it (more than higher educated)	(similar with the other groups above)	(similar with less digitally skilled)	Higher availability of OPS, ensure all services can be completed fully online, make signing up easy and fast

Figure 26 Vulnerable social groups' digital needs

5.3 Further analysis: The impact of biometrics

This section explores a more specific issue related to the IMPULSE solution, namely how the use of biometrics will affect how the IMPULSE solution is accepted. There are two main questions to be asked:

1. What impact, if any, is the use of facial recognition technology (FRT) likely to have on the acceptance of the IMPULSE solution?
2. What risks could the use of biometrics by the IMPULSE solution pose?

To explore the impact of biometrics on the acceptance of the IMPULSE solution, we asked survey respondents several questions. Firstly, as part of the survey, all respondents were shown a short video describing IMPULSE, and then asked whether they would use IMPULSE, were the solution available, instead of their current digital identity system. Respondents answered on a Likert scale ranging from 1 ("certainly not") to 5 ("certainly yes"). All who ticked 1 or 2 on the scale (which we may interpret as "certainly or probably not") were then asked a further question, namely why they would not use IMPULSE. They were offered a menu of six predefined answers to choose from, with instruction to pick *all* that applied, plus an "Other" option with a free text box to specific their "Other". One of the predefined options was "I am worried about facial recognition".[22] Figures 26 and 27 present the results from the two questions.

As Figure 27 illustrates, the survey results show that for about 43 percent of those survey respondents who did *not* want to use IMPULSE (73 out of 170), distrust of facial recognition was a motivating factor. This represents about 10 percent of the *total* population of respondents. Conversely, for 57 percent, (distrust of) FRT evidently was *not* a factor motivating their non-acceptance of IMPULSE. This suggests that FRT has a relatively small disuasive impact on acceptance of IMPULSE: for a relatively small section of the population, it is at least one factor motivating non-acceptance, but for most, it does not matter. This is broadly consistent with prior literature, which has found that privacy concerns and distrust of facial recognition is an important factor leading subsets of the population to reject technologies based on facial recognition (e.g. Liao et al. 2022, Kostka et al. 2021).

[21] This is in particular user name and password.
[22] For the further answer options, see Figure 27 below.

To further explore the factors behind (non-) acceptance of facial recognition, we asked respondents whether they had used any of the following authentication technologies: username and password, Smartcard and PIN, PIN/TAN systems, fingerprint recognition, facial recognition, voice recognition, and eye (iris) recognition. We next asked them to indicate their preferred, top-three of these authentication technologies, and then conducted statistical analysis of this data. Figure 28 presents the responses.

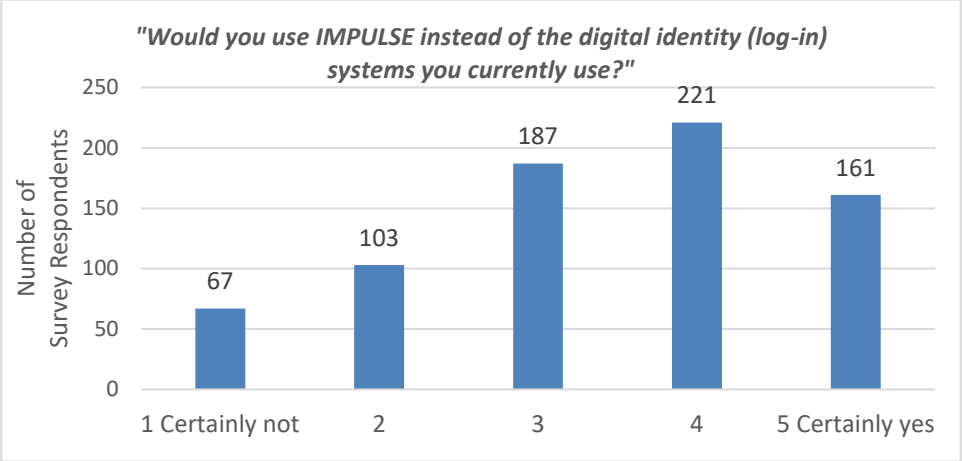

Figure 27: Intention of using IMPULSE

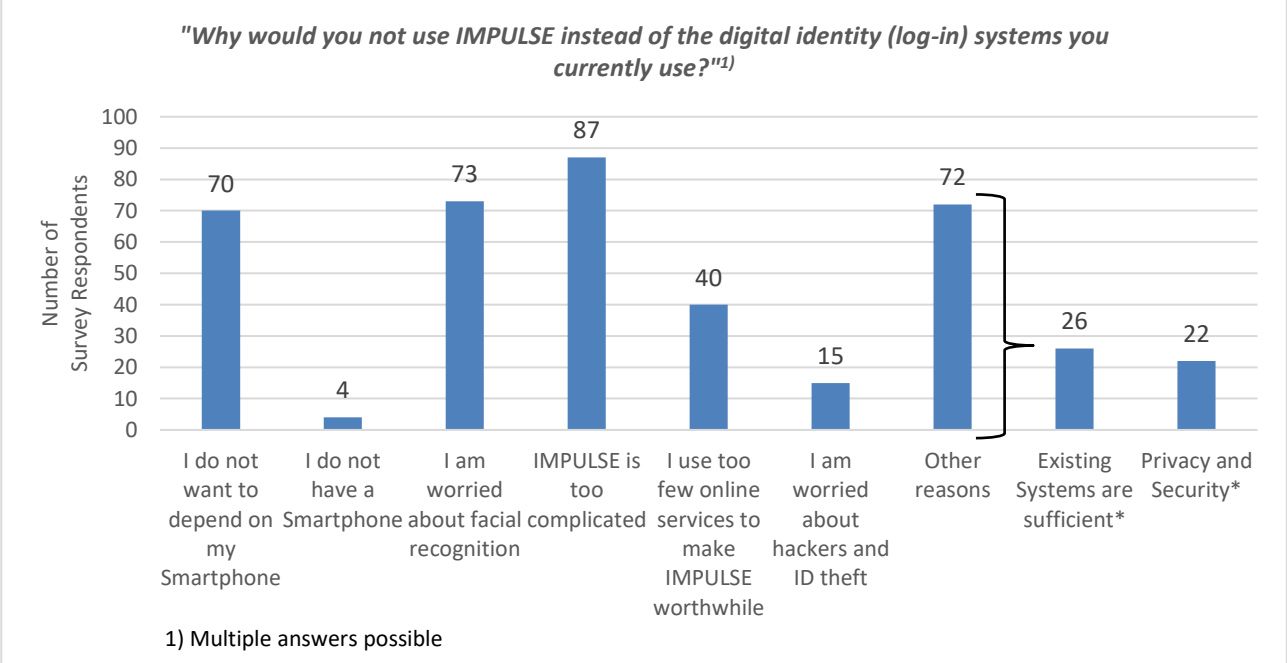

Figure 28: Reasons for not using IMPULSE

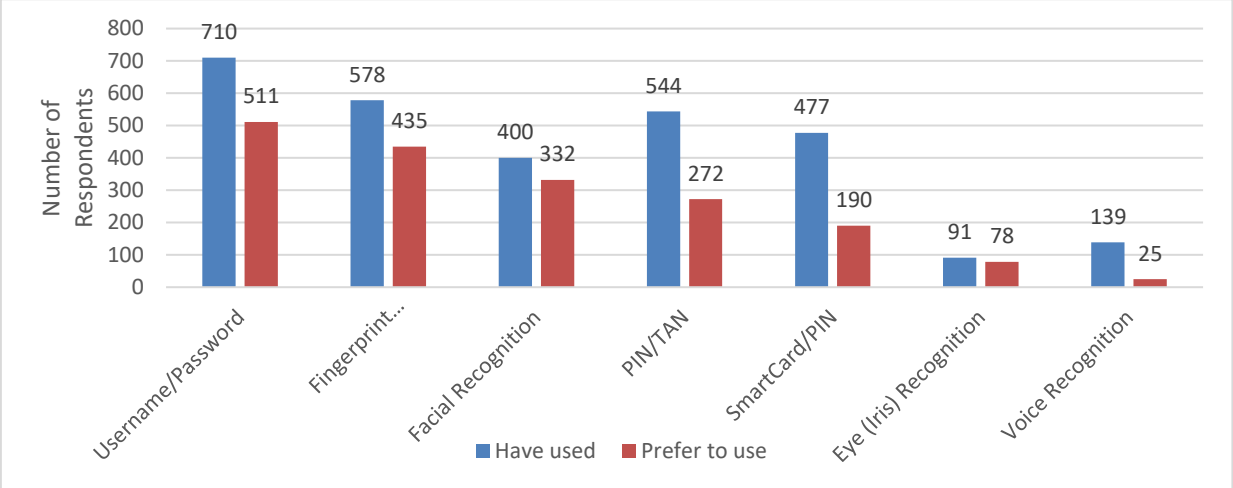

Figure 29: Used and preferred authentication technologies

Evidently, username and password remain the preferred authentication technology, followed by fingerprint recognition. In third place comes facial recognition. Strikingly, the gap between the number of have used and who would prefer to use FRT is among the second-smallest of all the technologies surveyed, with only 9 percent of those surveyed. This suggests that many respondents who have experience with using FRT may be keen to use it future, something also borne out by the statistical analysis presented below. By contrast, the gap between "have used" and "prefer to use" is rather larger for username/password (27 percent), Smartcard/PIN (39 percent) and PIN/TAN (37 percent): while large majorities of respondents have experience using these technologies, many who have this experience would seem to prefer to *not* use these technologies in future.

To explore the determinants of preference for facial recognition, we regressed this preference on a battery of independent variables. These are:

- age (variable name is "zus_Alter" in the regression table shown below)
- sex ("GeschlechtMale", a binary variable with 1 = male[23])
- education ("Schulbil1" [completed secondary school, vocational training or in vocational training] and "Schulbil2" [completed or in higher education])
- country ("Land_label_selSmallDE-FR-IS", a dummy variable discussed further below)
- experience using FRT ("NutzDigID_61"), a dummy variable with 1=usage experience
- experience using fingerprint recognition ("NutzDigID_51"), a dummy variable with 1=usage experience
- experience using *any* biometric recognition *except* facial (i.e., fingerprint, voice or eye/iris ["NutzDigID_oth_facial…"), a dummy variable with 1=usage experience
- Privacy concern ("zus_DatenSch", an ordinal variable ranging from 1=little concerned about privacy online to 5=highly concerned about privacy online)
- Openness towards new technologies ("zus_NeueTech", an ordinal variable ranging from 1=little interested in trying out new technology, to 5=very interested in trying out new technology)

In prior model specifications (not shown here) we also included household income, which was not significant in any specification, and dummies for individual countries (Germany, Italy, etc.), which showed interesting patterns we return to below.

The results are shown in Figure 30. The first model only regresses usage preference on age, sex, education, privacy concern and openness to new technologies. Age is weakly significant, with a negative sign, but this significance goes away in the following models, as further controls are added. Sex and education are never significant. Privacy concern is weakly significant, with negative sign; technology openness highly significant, with a positive sign.

[23] In the survey itself, we gave respondents the option of "non-binary", besides males and female, as well as "other". However, only a miniscule number chose to describe themselves thus.

In model 2 we add the country dummy. This is set to 1 if the respondent is from Germany, France or Iceland, and 0 if they are from other countries. The reason for this seemingly curious variable is that in prior regressions (not shown here) country dummies for these countries had been significant. For simplicity of presentation, we have therefore grouped these countries together in one variable in these models. The country variable is highly significant (99th percentile), and remains so in all further models, except the last model (model 8). Evidently, substantial segments specifically of the German, French and Icelandic respondents prefer *not* to use facial recognition. Interestingly, now that country is controlled for, the significance and effect size (coefficient size) of privacy concerns rises. It remains significant at the 95th percentile through all further specifications, except the last model. In the last model, we add an interaction term between the country and the privacy concerns variable. ("Land_label_selSmallDE-FR-IS:zus_DatenSch"). The interaction term is weakly significant and negatively signed. The privacy concerns variable loses significance and much of its effect size (coefficient size) is lost. The country dummy also loses significance, and even changes sign: it now becomes *positive*.

German, French and Icelandic respondents are disproportionately hostile to facial recognition compared to respondents from other countries. This concern is related to general privacy concerns.

We interpret these results to suggest that German, French and Icelandic respondents are disproportionately hostile to facial recognition, compared to the respondents from the other countries, and (2) that this concern is related to general privacy concerns, but (3) that this relationship between privacy concerns and hostility to facial recognition holds more strongly among the respondents from Germany, France and Iceland than those from the other countries. I.e., while Germans, etc., who have privacy concerns are also likely to be hostile to FRT, respondents from other countries who share the privacy concern may *not* also share the hostility to FRT. This again is consistent with prior literature, which suggests that Germans may be more sceptical of FRT than the residents of other countries (Kostka et al. 2021)

Results of all eight models

	Dependent variable:							
	zus_BevLogIn_5							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
zus_Alter	-0.011*	-0.008	-0.004	-0.003	0.0003	0.001	0.001	0.001
	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)
GeschlechtMale	-0.010	-0.048	-0.042	-0.043	0.041	0.040	0.040	0.038
	(0.178)	(0.180)	(0.183)	(0.183)	(0.197)	(0.197)	(0.197)	(0.197)
Schulbil1	-0.112	-0.073	-0.130	-0.120	-0.130	-0.134	-0.132	-0.114
	(0.418)	(0.422)	(0.426)	(0.426)	(0.453)	(0.453)	(0.453)	(0.455)
Schulbil2	0.286	0.410	0.381	0.384	0.418	0.416	0.413	0.416
	(0.330)	(0.335)	(0.337)	(0.338)	(0.357)	(0.357)	(0.357)	(0.359)
Land_label_selSmallDE-FR-IS		-0.729***	-0.677***	-0.649***	-0.770***	-0.761***	-0.752***	0.540
		(0.188)	(0.190)	(0.190)	(0.203)	(0.203)	(0.204)	(0.717)
NutzDigID_oth_facialUse of other biometric			1.033***			0.162		
			(0.279)			(0.313)		
NutzDigID_51				0.980***			0.189	0.219
				(0.261)			(0.292)	(0.292)
NutzDigID_61					1.748***	1.707***	1.699***	1.696***
					(0.199)	(0.214)	(0.213)	(0.213)
zus_DatenSch	-0.156*	-0.208**	-0.187**	-0.195**	-0.207**	-0.204**	-0.205**	-0.062
	(0.085)	(0.088)	(0.089)	(0.089)	(0.095)	(0.095)	(0.095)	(0.121)
zus_NeueTech	0.303***	0.287***	0.225**	0.225**	0.139	0.133	0.131	0.120
	(0.094)	(0.095)	(0.098)	(0.098)	(0.104)	(0.105)	(0.105)	(0.105)
Land_label_selSmallDE-FR-IS:zus_DatenSch								-0.366*
								(0.196)
Constant	-0.652	-0.350	-1.214*	-1.143	-1.127	-1.245	-1.258*	-1.755**
	(0.654)	(0.668)	(0.717)	(0.712)	(0.724)	(0.760)	(0.753)	(0.800)
Observations	567	567	567	567	567	567	567	567
Log Likelihood	-378.631	-370.881	-363.330	-363.250	-328.189	-328.053	-327.977	-326.209
Akaike Inf. Crit.	771.263	757.761	744.659	744.500	674.378	676.106	675.954	674.417
Note:								*p<0.1; **p<0.05; ***p<0.01

Figure 30: Regression results

In models 3 to 5 we further, respectively, the variables for having used a biometric authentication technology other than FRT ("NutzDigiID_oth…", model 3), for having used fingerprint recognition ("NutzDigID_51",

model 4), and for having used FRT ("NutzDigiID_61", model 5). In models 6 and 7 we keep the variable for having used FRT, and one of the other two. The bottom line is that the prior-use-of-FRT-variable is highly significant and positive, with a very strong effect size, and remains so under all specifications. However, when this FRT-variable ("NutzDigiID_61") is added, the other two variables cease to be significant (models 6 and 7). We interpret this to mean that **respondents who have prior experience with using FRT tend to prefer to use FRT also in new solutions (like IMPULSE).** In other words, for respondents who have used FRT in the past, this experience seems mostly to have been positive, and this past positive experience of FRT encourages them to prefer continuing to use FRT.

Respondents who have had positive experiences with the use of facial recognition technologies in the past are more likely to use such technologies in new solutions such as IMPULSE. Their positive experience seems to encourage them to use such technologies.

Conversely, experience with using fingerprint, voice or eye/iris recognition *by itself* does *not* cause respondents to wish to use FRT in future. This is significant in as far as many respondents have evidently had positive experiences with these other biometric authentication technologies (Figure 29). In other words, positive experience and usage inclination does *not* travel *between* different biometric technologies: that I have had positive experiences with, for example, fingerprint recognition, by itself does not make me more inclined to use FRT. That the variables for the other biometric authentication technologies were significant when experience with FRT was *not* controlled for (models 3 and 4) most likely reflects that many respondents who have used FRT had also used the other biometric technologies. It is also notable that once the experience of using FRT is controlled for (models 5 to 8), the technology openness variable ceases to be significant and its effect-size declines. We interpret this to suggest that people who score high on technology openness tend to be early adopters of new technology, and have thus mostly had prior experience with FRT.

Summing up, the regression results and the foregoing qualitative analysis suggest:

1. Firstly, that while **FRT is a strong impediment to the acceptance of IMPULSE** for some people, this is quite a small group.
2. Secondly, this group may be concentrated more in certain countries than others, **especially in Germany, and possibly France and Iceland**.
3. Thirdly, **prior (positive) experience with using a technology is a very important factor** driving future usage preferences. However, as the low preferences for continuing to use PIN/TAN and Smartcard/PIN systems indicates (Figure 29), prior usage experience is not by definition perceived as positive.

While these results strongly suggest that there is a "market" for FRT-based authentication systems like IMPULSE, what of the potential risks? Legally speaking, under the GDPR biometric data "for the purpose of uniquely identifying a natural person" belong to a "special" category of personal data, for which particularly strong controls are mandated (GDPR Art. 9). Thus **it is only legal to process this data if the data subject has given explicit consent (Art. 9(2)(a)). This is the case in IMPULSE.**

More generally, the increased use of biometric data across society, state and economy comes with a range of potential risks and benefits. Among the risks are increased information and power asymmetries between citizens and states and corporations, the "chilling effects" (self-censorship) this might encourage in citizens, the danger of "false positives"/"false negative"-type errors in imperfect systems, and in particular the risk of increased, hard to detect identity fraud ("deep fakes") and ensuing broad collapse of trust in society. Among the potential benefits are a wide range of cost savings, better policing and greater security, a viable substitution for password-based authentication systems and greater economic growth.[24]

Especially in Europe, there seems to be a "market" for FRT-based authentication systems. Here, the legal and institutional data protection infrastructure provided by GDPR mitigates some of the risks commonly associated with using biometrics. Furthermore, IMPULSE itself mitigates some of these risks, as it is designed to allow the

[24] For a general discussion of risks and benefits see Karaboga et al. (2002)

user to technically hide their biometric data from the service provider. However, there is still a risk of power imbalance, meaning service providers tend to ask for more personal data than necessary for the service. This must be addressed at a policy level.

It should be noted that **many of the most severe risks are somewhat general in nature. In other words, they derive less from any single use case or system (such as IMPULSE)** than from the possible larger changes that could be prompted by the widespread deployment of FRT in many different systems, use cases and circumstances.

With regard specifically to IMPULSE, in this regard the risks the systems could create seem quite modest. The most important reason for this is that the biometric data processed in IMPULSE is stored *only* on the device of the IMPULSE user herself. The **service providers (be they public or private) as well as the entity providing and running the IMPULSE system, do *not* retain access to or control over this data. This dramatically reduces the risk of it being misused or used in ways that stretch or exceed the original purpose.** A residual risk that these (or other) entities might manipulate ("hack") the IMPULSE system to retain the data illegally and/or in contravention to the IMPULSE terms of service and data usage/data protection agreements of course remains. However, at least in Europe this risk seems fairly low, due to the existence of a quite highly developed legal and institutional data protection infrastructure in form of the GDPR and related regulations, and the data protection authorities and officers, as well as critical media and civil society organisations. In other world regions this is likely to be different, though it is worth noting that globally, data protection regulations and infrastructure are increasingly following the GDPR.[25]

A greater risk than (mis-) use of biometric data *in contravention to* the usage and data protection agreements, however, is that service providers exploit their power vis-à-vis users to compel them to hand over more data than they would like to or is strictly necessary for the service provided *as part of* the usage and data protection agreements, including the biometric data stored on their devices. As argued in greater detail in Martin (2023), this risk is a structural feature of SSI (and other digital identity systems) that comprise a digital wallet containing diverse "interesting" data points, such biometric information or certificates and verifiable credentials of various kinds. **While SSI systems like IMPULSE mean that the user has to actively consent to every data request by a service provider, the power asymmetries of the digital economy mean that users often have limited scope to refuse service providers' data requests.** Service providers can and often do present users with "take it or leave it"-offers, where they need to either consent to the data request and associated data processing, or forego access to the service in question. What makes the wallet feature of SSI systems unique and structurally different to traditional digital identity systems, is that it serves as a point of storage and of access to many different, potentially valuable data. By themselves, SSI systems (including IMPULSE) provide few safeguards to stop malevolent or simply curious service providers making service provision conditional upon access to and transfer of all manner of data stored in the wallet – including the biometric data. Far from safeguarding user privacy and sovereignty, SSI systems thus have the potential to turn into "disclosure machines" (Martin 2023) that systematically work to make more data available to service providers, including more biometric data, than users might want. Indeed, because this power of service providers derives from the structural features of the digital economy and involves the (arguably coerced) "consent" of the user, SSI systems like IMPULSE are structurally ill-placed to remedy this problem. The remedy must come from larger legal, political and institutional safeguards on the societal level, rather than the technical safeguards on the system level that SSI solutions can offer.

Again, in Europe the GDPR and the wider data protection infrastructure already provide fairly effective safeguards against such (semi-coerced) excess data disclosure. **Forcing users to provide additional data beyond what is needed to provide the service runs counter to the GDPR's principles of purpose limitation and data minimisation (Art. 5(1)(b) and (c)), and are thus generally illegal.** These risks would be more pronounced were the IMPULSE solution to be made available outside of Europe. At present, however, this is not under discussion.

[25] See e.g. Wu and Hayward (2023)

6 Adoption factors in the IMPULSE pilot cases

As part of WP4.1, our main KPI was formulated in the following way: *Identify a set of approximately three to five scenario-specific factors that drive the adoption of new eID solutions among different stakeholder groups, to be specified for each case study pilot in which the IMPULSE eID solution is implemented.*

The six IMPULSE pilots are therefore analysed against the above KPIs in this chapter. The results that are presented here are based on additional interviews that we did before the start of the pilot cases. The WP2 experts (responsible for the pilot cases) also checked whether the adoption factors we identified in WP4 still applied after the pilot cases.

Adoption is the process of integrating new digital solutions into an organisation's daily operations, while acceptance refers to the immediate use of an eID solution and individual user behavioural intentions (see Jackwerth-Rice et al., 20239. This means that adoption refers to the reasons *why other organisations should adopt a new eID solution to access online services*, which could then contribute to the diffusion of such a solution.

In order to identify such factors of adoption for each of our pilot cases, we have applied a framework that specifies adoption factors with respect to blockchain technology (see Janssen et al. 2020). We have chosen this framework because it covers institutional, market and technical factors which are all relevant in the pilot cases. The three dimensions are shortly specified below.

- **Institutional factors**: This dimension refers to those *norms and cultures* that shape how organizations who can be incumbents or new to the field interact with each other (service provider, partners, users etc.) or how new digital technologies are *regulated* or *governed*.
- **Market factors**: This dimension include issues such as how the *market is structured* in which an organization operates. This also includes how (public) organization make *contracts or agreements* to buy and sell products or services and how they organize their *work or processes* to create value.
- **Technical factors**: This dimension includes issues such as *information processing time* or *security risks* with regard to the design of the system, cybercrime or newness. It may also include question of a *shared infrastructure* or *technical standards* for services.

For each IMPULSE pilot cases, we have derived the following adoption factors.

	Aarhus	**Reykjavik**	**Ertzaintza**	**Gijón**	**Unioncamere / IC**	**Peshtera**
Institu-tional factors	Social inclusion (here also access of VC such as homeless) State takes responsibility for access Services are used as intended	Social inclusion of VC, such as people with disabilities	Digitization of state-citizen interactions Easier access to insurance benefits	Social inclusion of formerly ex-cluded social groups		Social inclusion (e.g., elderly, less digitally skilled) Proven solution for trustworthy online services
Market factors and processes	Reducing extra-work in re-acquirement of personal documents		Efficiency gains in the handling of complaints Facilitation of law enforce-ment	Greater control of registered individuals Personalization of access and services (legal status, place of residents)	Efficiency gains in both the usage and the onboarding process	Efficiency gains for citizens

				More sensitive services possible		
Technical factors	No relying on a digital device (which can be lost or sold)	Easier and trustworthy access based on facial recognition		Interoperability with other local authori-ties (rather speculative)	Limit fraud or misuse of data and informa-tion Portability of IMPULSE ID for accessing other contexts in IT and EU	Proven solution for accessing national service plattform

Table 6 'Good' reasons for adopting IMPULSE

City of Aarhus (Denmark): In this case, it is about the electronic access to lockers in which people can store personal documents and key cards to access public services. The Municipality's Citizen Service Centre, including the staff who manage these lockers, are the most important organisations (stakeholders). Apart from that, the shelters are also important. They have an interest in taking care of VC.

- Other organizations could actively contribute to the political objective of providing *full access* to public services for all including *vulnerable citizens*. This could also potentially be used by other social groups wishing to keep personal documents securely stored.
- State authorities would also take *responsibility for providing access to public services* to all citizens. This is done by centralising access points to services (lockers) which means that the state takes responsibility for providing the technical infrastructure for VC (they do not rely on digital devices).
- They could help to make sure *public services are used as intended*. This could help vulnerable citizens to engage with public services earlier and more often and to make better use of their social rights. This also means that VC comply with the rules and law (e.g., no illegal keeping of ID cards at the shelters).
- They could *reduce the amount of extra work* caused by the loss of personal documents or identity cards. In particular, in the past, social workers, such as those working in shelters, have compensated for such losses by assisting in the process of re-acquiring them.

City of Reykjavik (Iceland): In this case, the City of Reykjavik was particularly interested in facilitating access to its "Better Reykyavik" participatory democracy portal for every citizen, incl. socially marginalized group. On this platform, Icelandic citizens have the opportunity to access all government services to which they are legally entitled. The platform is part of an active democracy in Iceland. It enables citizens to influence decisions in their neighborhood (changes, prioritization of resources, feedback, political decision-making processes.

- A key adoption factor was assumed to be a technical one, i.e. offering people with physical disabilities in particular an alternative, but *easier and trustworthy access* to the platform compared to the already established forms of access, e.g. via facial recognition instead of entering a phone number and memorizing a password. This vulnerable group includes people with cerebral palsy or varying degrees of lack of control over their limbs.
- In addition, this technical factor could also contribute to the overarching policy objective of *social inclusion*, i.e. to enable vulnerable social groups to have easy access to Icelandic online services and to facilitate their participation in local policy-making processes that take place online.

The pilot did not show that the IMPULSE solution was more user-friendly. In fact, the Better Reykjavik platform was discontinued during the project and instead IMPULSE was compared with the current eID system in use in Reykjavik. After the pilots, the IMPULSE solution did not prove superior to the current eID solutions in Iceland and the solution as a whole was not considered superior to existing solutions.

However, the pilot case participants were interested in facial recognition and felt it could be used for better eID solutions for vulnerable citizens. The IMPULSE solution is therefore competing with other eID solutions

as well as facial recognition software and it might be a technical lever for social inclusion, as in the case of the City of Aarhus.

Ertzaintza – Law Enforcement Agency (Spain): This case deals with the issuing of complaints entirely online. It has the potential to digitize interactions between the state (police authorities) and citizens. In the past, these interactions were usually conducted in person. One of the main interests of the police authorities (25 in the pilot region), which is directly related to this case, is the recording of minor crimes and the reduction of workload. Therefore, only if the digitized interactions actually make it easier for both the police and citizens to report, will the adoption factors mentioned below apply. This was only partially tested in WP2, as the participants were mainly employees of the Ertzaintza Police Department and not ordinary citizens.

- The main driver for adoption is potential *efficiency gains*. Minor offences, which have so far largely had to be recorded in person, account for over 90% of reports. This would be a key driver for adoption if digital solutions resulted in such reports being largely error-free and without the need for much investigation.
- Other factors for adoption are more likely to be suspected. For police forces, the *facilitation of law enforcement* is certainly the main interest. Therefore, making it easier to report such offences and thus increasing their visibility may also be in the interest of other police forces.
- From a government perspective, other adoption factors arise. Such solutions could also contribute to the *digitization of government-citizen interactions*, which have so far been largely face-to-face (the online procedure already in place is hardly used). Such solutions could raise awareness regardless of age group (old, young) and place of residence (urban, rural).
- From the state's point of view, another reason could be to make it easier for citizens to *access insurance benefits*. Compensation is only paid if the citizen reports the incident, which must be done within 72 hours.

However, it must be emphasized in this case: It remains to be seen, even after the pilots, whether this solution will actually bring about the hoped-for increased efficiency. It is even conceivable that this could even lead to additional work (correcting applications, contacting applicants, applicants still seeking personal contact).

Gijón Municipality (Spain): Currently, the City of Gijón offers its residents and visitors various online services, e.g. transport, parking, libraries, museums, car sharing, census, enrolling in courses, making payments, etc., which are accessible using a citizen card or a citizen application ("Gijón App"). The city's main interest is to have more citizens to use these services. Although different means of identification are already quite well established, some factors could be reasons in favor of introducing IMPULSE as additional eID solution.

- At the moment, also visitors to the city as well as legal persons (companies, schools) can register for services. With the help of an IMPULSE solution, the city administration could have *greater control over who is actually registered* (place of residence, legal status).
- The personalization of access could also open up the possibility of offering *more sensitive services* in the future, such as voting. This will only be possible if the IMPULSE solution proves to be easy and secure during the pilot tests.
- From the point of view of municipalities that wish to spread the usage of public services, there may be (even) more usage by groups of the population that have not used them much so far, because it is easier to register.
- Another factor could be *interoperability with other local authorities* (towns, villages). Other municipal administrations in the region could also implement IMPULSE, so that visitors from other municipalities would not have to re-register in order to make use of the local services. However, the experts regard this factor as rather speculative.

In this case, there is little evidence that the solutions have had an inclusive effect. The main aim of IMPULSE was to test ways in which the city could have more control over registrants and thus introduce more sensitive services.

Unioncamere | InfoCamere (IC) (Italy): In this case, the main interest is to facilitate entrepreneurs having access to public and private services. The central actor is the Italian Chamber of Commerce, which provides access to these services and, for this purpose, offers a "digital drawer for enterprises". However, entrepreneurs, who may be Italian or foreigners, register through already quite well-established national e-ID system (SPID) or apply for a CNS card / token from the Chamber of Commerce. For this case, the following reasons could be derived why IMPULSE might be adopted also by other organizations - only the first and second were mentioned during the pilot cases. The last remains potential.

- For the Chamber of Commerce *efficiency gains* might be a central adoption factor. In the future, the registration (*onboarding process*) could be handled by the IMPULSE solution so that authorities do not have to check new identities manually.
- In the long term, the *portability of IMPULSE identities* - to access other public and private *contexts* in Italy or the European Union - is key to adoption. For example, it is conceivable that entrepreneurs could use their wallet identities for registration in the national business register.
- If IMPULSE proves to be a solution that can better prove an individual's identity by storing multiple credentials in the wallet, it could also *limit fraud or misuse of data and information* assigned to individual companies and accessible through the portal. This wallet functionality is not yet included in established eID systems.

Municipality of Peshtera (Bulgaria): In this case, the main interest is to provide Bulgarians with an easier access to an online platform for services that was launched by the government in 2021. Through this platform, the municipality of Peshtere offers a range of online services. Most of them involve issuing certificates (birth, inheritance, marriage, re-registration, etc.). Currently, citizens use these services with an electronic signature which they obtain from an authorized private provider and which they can also use for other services (banking, taxes). For this case, the following adoption factors could be relevant.

- *Efficiency gains for citizens* (in particular young people and families), as they no longer need to apply in person to a private service provider for access (via the e-signature). By removing the fees for issuing an e-signature, IMPULSE can provide further financial incentives.
- Currently, very few Bulgarians have applied for an e-signature. The process of applying for a new e-signature is perceived by the case experts to be rather complicated. It could therefore be an important *social inclusion* objective for the municipality (e.g. elderly people, the less digitally skilled) to provide an easier access to them.
- If the Peshtera case also *proves to be a trustworthy solution*, this could be a main adoption factor. Given that data misuse in the past has severely damaged citizens' trust in online services, IMPULSE might promote adoption if it has demonstrated secure handling of personal data.
- Similarly, another rather long-term adoption factor could be that IMPULSE has proven to be a solution for accessing the *national service registration* which might than be adopted by other national and local authorities.

7 Conclusions

Within the IMPULSE research project, WP 4.1 concentrated on providing empirical evidence on how to both strengthen DI in Europe and promote the uptake of eID management solutions like IMPULSE itself. We started our analysis with the assumption that the level of DI **varies significantly across Europe**, due to the impact of the different welfare states (Alexopoulou et al., 2022).

We tried to identify why levels of digital inclusion and exclusion might differ across Europe, both in terms of **social and cultural factors**. In addition, by taking a closer look at the digital needs of vulnerable social groups, we tried to thoroughly assess how IMPULSE as a technology could contribute to DI. This chapter summarizes our empirical findings and critically reflects on them in the light of the results of our expert consultation whose main results are summarized in table 2 and 3.

7.1 Social factors of DI

With regard the social factors, our results show that age and **digital skills**, but also **technology affinity** could be considered as key factors of DI / DE. [26] Our observation that **age**, but more importantly digital skills points to the ability to use digital solutions is a key factor: the easier to use an eID solution, the lower the digital skills required for all social groups.

In the context of the development of eID solutions, however, this supposedly linear relationship cannot be directly implemented. Ultimately, it remains a **risk assessment carried out in innovation project** to find the right balance between regulatory security requirements and the user's interest in easy-to-use technologies, as one expert pointed out below.

> *"It means: You are here in terms of regulation. There are a number of areas where we may not comply with all the details of the law. So a high level of security is required by government lawyers and government security officers. So from my side, I'm in business development, I try to find the right balance. Our view is that convenience and ease of use are much more important than a certain level of fraud risk in some cases" (expert consultations).*

The above quote also points to other institutional factors to explain the DI process. These include **regulation** and the **capability to interpret the rules** in terms of multiple interests and digital needs, especially those of citizens and users. This emphasis on non-technical factors as an explanatory factor for digital exclusion or inclusion is consistent with findings from other expert consultations, as the other mentioned below shows.

Other non-technical factors discussed in the interviews relate to **personal routines** of searching and access information, **personal networks** (peers, grandchildren, etc.), **information channels** and **social points of contact** through which people learn about government services, such as local municipalities, universities, schools, kindergartens, trade unions, associations, churches, etc.

> *"We have observed that the importance of technological barriers has been declining over time. (...) Conversely, non-technical elements, such as trusting services and public institutions, as well as policies for managing data, have become more important" (expert consultation).*

Our conclusions appear to be in line with the conclusions of other studies on the acceptance of e-government services in Germany, Austria and Switzerland, where non-technical factors such as **lack of awareness** of the online availability of government services and **intentional offline use** are identified as key factors in the digital divide in the use of online services (TUM & Initiative D21, 2022).

Our findings are also consistent with research highlighting that informing citizens about their social rights on the web, and how to exercise and enforce them, could increase trust in government services and reduce digital inequalities which are considered as important drivers of digital inclusion (Robles et al., 2021).

[26] This might be in line with the EU strategy to build up digital skills: https://www.europarl.europa.eu/news/en/press-room/20220516IPR29661/meps-back-path-to-the-digital-decade-roadmap-for-2030.

7.2 Cultural factors of DI

With regard to the cultural factors we tried to look more closely at the institutional contexts that are conducive to DI. We found that being a citizen of a conservative or Eastern European country appear as key factor of DI. Moreover, our results suggest that **social democratic and southern European welfare regimes minimize the risk of DI** more than the other welfare regimes. While the results for southern Europe and conservative countries, especially Germany, surprised us, the high level for social democratic countries supported our assumption.

Perhaps the institutions and policies of social democratic (but maybe also Southern European countries) are more likely to minimize the risk of digital exclusion.

Another cultural driver of DI emerged from our analysis which points to the **capabilities of public sector organizations**, such as agencies or municipalities, and their ability to actually provide a wide range of online services for all social groups that are at risk of digital exclusion. This might imply a cultural change within state authorities as one expert pointed out.

"One big problem we have is that we need to change how we work in the government. (...) We now have a government-centric administration, which is very bureaucratic. We need to move to a citizen-centric administration, which is always actively listening to citizens and users. It involves citizens in designing, co-creating and prototyping to deliver the best services. This is a major shift in the way we currently deliver public services. It is a very important step in the development of citizen-centered government. If we do this and adopt a citizen-centered strategy, everything else will follow" (expert consultation).

On the basis of our discussions with the experts, we are able to specify these new capability requirements for public sector organizations in a little more detail. It means:

1. Putting **social inclusion** of specific social groups on the political agenda (e.g. integration of foreign skilled workers or experts, refugees or people with disabilities) before discussion of technologies.

2. The state takes **full responsibility** for ensuring that all social groups have access to their online services, e.g. if access is only allowed via private devices, new risks of exclusion arise.

3. Definition of **usability requirements** with regard to social groups, e.g. simple forms that are easy to find, simple language, translations into English or other languages, 24/7 support, etc.

4. Enhancing **trust in government** services through technical design (e.g. cybersecurity or protecting against identity theft).

We believe that these capabilities are part of a larger challenge to the state to become more of a problem solver. This challenge is discussed in the research literature on socio-technical change (see also Borrás/Edler, 2020).

7.3 IMPULSE' contribution to digital inclusion

With regard to our third objective, we found that, in general, **all participants seemed to be very receptive to IMPULSE.** In fact, IMPULSE may encourage some social groups to use public services more often. This is particularly the case if their main concern is to retain control over their personal data. However, we found little evidence to assume that IMPULSE might contribute to greater digital inclusion in Europe.

Our findings suggest that IMPULSE is only addressing some of the digital needs of those social groups that are likely to be digitally excluded from using OPS.

As far as the technical solution of IMPULSE is concerned, here are our conclusions in a nutshell.

- IMPULSE could be a technical intervention to support DI in Eastern Europe, but there is no clear evidence for the other European welfare regimes.
- Still to be evaluated for IMPULSE, trustworthiness and ease of use (ideally as easily as for private services) are key factors for acceptance/adoption, as age and digital skills seem to be relevant.
- IMPULSE itself may have little impact on DI in Europe, but non-technical factors could be more important, e.g., digital skills, higher availability of OPS, higher awareness of new OPS.
- Politically prioritize reducing non-technical barriers such as trust and awareness as well as targeted information campaigns for specific social groups, e.g., not only elderly, but also others.[27]
- PPP could be a main mechanism for an inclusive EU digital policy (in order to adopt already established and well-designed eID solutions for private services also for public services).

7.4 Inclusive digital policy

On the basis of our study, we propose to understand the problem of DI first as a problem of social inclusion, with a focus on the utilization of social rights that people have within the EU, regardless of their origin or socio-demographic background. A key DI issue is ensuring that all people can exercise their **social rights in both digital and analogue worlds,** wherever they work and live in the EU and whichever public service they use, online or offline. This approach to DI reformulates the research objectives:

- Which social rights and of which social groups are strengthened or undermined by the digitization of public services?
- Which digital technologies are best suited to enhance social rights for all EU citizens, regardless of origin or socioeconomic status?

This points to an alternative policy approach to DI which was stressed in our expert consultations. The experts pointed out that an EU digital policy that understands digital inclusion as a social inclusion issue must focus on the social rights of marginalised groups, rather than a technology-centered approach.[28]

Such a policy approach would then **integrate the needs of those social groups** that are most at risk of digital exclusion (e.g., foreign professionals, temporary residents, refugees), rather than promoting the diffusion of digital innovation. This policy approach also requires the **involvement of different 'communities'**, such as social inclusion, cybersecurity, etc., in the policy process of defining how public services are delivered online.

"I think the most important thing is to ensure that people can easily access public services online, as they can in the analogue world. The technology must then be designed in such a way that it does not create exclusion, but that basic rights are preserved and nothing is lost, but gained" (expert consultation).

Thus, digitizing the public sector is a matter of social policy. Based on our findings we suggest that the **Nordic countries could be a source of inspiration for a more inclusive EU digital strategy**. Their priorities for social justice and inclusion seem to translate into policies and institutions that are more effective in creating digitally inclusive societies.

[27] see TUM & Initiative D21 (2022)

[28] For example, in connection with the use of biometrics, which is at the heart of the IMPULSE solution, attention was drawn to new technology-induced risks of exclusion (identity theft). These should be taken into account before the technology is chosen.

References

Addo, A.; Senyo, P. K. (2021): Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion. In: *Government Information Quarterly* 38 (2), S. 101568.

Al Khateeb, A. (2017): Measuring Digital Competence and ICT Literacy: An Exploratory Study of In-Service English Language Teachers in the Context of Saudi Arabia. In: *IES* 10, S. 38.

Alexopoulou, S.; Åström, J.; Karlsson, M. (2022): The grey digital divide and welfare state regimes: a comparative study of European countries. In: *ITP* 35 (8), S. 273–291.

Aristei, David; Perugini, Cristiano (2012): Inequality and reforms in transition countries. In: Economic Systems 36 (1), S. 2–10.

Borrás, S.; Edler, J. (2020): The roles of the state in the governance of socio-technical systems' transformation. In: *Research Policy* 49 (5), S. 103971.

Ciesielska, Magdalena; Rizun, Nina; Chabik, Jakub (2022): Assessment of E-government inclusion policies toward seniors: A framework and case study. In: *Telecommunications Policy* 46 (7), S. 102316.

EP (2014): Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. 910/2014.

EP (2022): Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. Establishing the Digital Decade Policy Programme 2030. European Parliament (EP); Council of the European Union. Brussels.

Esping-Andersen, G. (1990): *The Three Worlds of Welfare Capitalism*, Princeton University Press, Princeton, NJ.

Esping-Andersen, G. (2015): Welfare regimes and social stratification. In: *Journal of European Social Policy* 25 (1), S. 124–134.

Ferrera, M. (1996): "The 'Southern model' of welfare in social Europe", *Journal of European Social Policy*, Vol. 6 No. 1, pp. 17-37.

Firke S. (2023): _janitor: Simple Tools for Examining and Cleaning Dirty Data. R package version 2.2.0, <https://CRAN.R-project.org/package=janitor>.

Gal, J. (2010): Is there an extended family of Mediterranean welfare states? In: *Journal of European Social Policy* 20 (4), S. 283–300.

Gohel D.; Skintzos P. (2023): _flextable: Functions for Tabular Reporting_. R package version 0.9.3, <https://CRAN.R-project.org/package=flextable>.

Hatos, A.; Cosma, M.-L.; Clipa, O. (2022): Self-Assessed Digital Competences of Romanian Teachers During the COVID-19 Pandemic. In: *Frontiers in psychology* 13, S. 810359.

Hlavac, M. (2022): stargazer: Well-Formatted Regression and Summary Statistics Tables. R package version 5.2.3, https://CRAN.R-project.org/package=stargaze.

issa (2022): Leaving no one behind: Experiences in digital inclusion from Europe. Ed: *issa* Excellence in Social Security. Online available: https://www.issa.int/analysis/leaving-no-one-behind-experiences-digital-inclusion-europe, last checked: 1st of Oct 2023.

Jackwerth-Rice, T., Martin, N., Silvestru, D., Pullmann, L. & Blind, K. (2023): *Report on social perception and recommendations: Deliverable D4.1 (V1)*. Research project IMPULSE 'Identity Management in PUbLic SErvices'. Brussels.

Janssen, M.; Weerakkody, V.; Ismagilova, E.; Sivarajah, U.; Irani, Z. (2020): A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. In: *International Journal of Information Management* 50, S. 302–309.

Kammer, A., Niehues, J. and Peichl, A. (2012): "Welfare regimes and welfare state outcomes in Europe", *Journal of European Social Policy*, Vol. 22 No. 5, pp. 455-471.

Karaboga, M., Frei, N., Ebbers, F., Rovelli, S., Friedewald, M., and Runge, G. (2022): Automatisierte Erkennung von Stimme, Sprache und Gesicht: Technische, rechtliche und gesellschaftliche Herausforderungen. TA-SWISS 79/2002, https://doi.org/10.3218/4141-5.

Kostka, G., Steinacker, L., Meckel, M. 2021: "Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States", Public Understanding of Science, Vol. 30(6) 671–690, DOI: 10.1177/09636625211001555.

Liao M., Agnihotri D., Zhong, X. 2022: "'Paying with my face' -- Understanding users' adoption and privacy concerns of facial recognition payment", Proceedings of the 2022 HFES 66th International Annual Meeting, 731–735, DOI: 10.1177/1071181322661480.

Martin, N. 2023: "The Chimera of Control. Some Critical Reflections on Self-Sovereign Identity". Paper presented at the fifthteenth interdisciplinary workshop on "Privacy, Data Protection & Surveillance", 18 July 2023, Alexander von Humboldt Institute for Internet and Society, Berlin.

Mossberger, K., Tolbert, C.J. and Stansbury, M. (2003): *Virtual Inequality*: Beyond the Digital Divide, Georgetown University Press, Washington, DC.

Nguyen, A.; Hong, Y.; Gardner, L. (2020): *A Taxonomy of Digital Learning Activities for Digital Inclusion*.

Pérez-Amaral, T.; Valarezo, A.; López, R.; Garín-Muñoz, T. (2021): Digital divides across consumers of internet services in Spain using panel data 2007–2019. Narrowing or not? In: *Telecommunications Policy* 45 (2), S. 102093.

Petmesidou, M.; Guillén, A. M. (2022): Europe's green, digital and demographic transition: a social policy research perspective. In: *Transfer: European Review of Labour and Research* 28 (3), S. 317–332.

Renda, A.; Iacob, N.; Campmas, A. (2021): Study supporting the final evaluation of the programme on interoperability solutions for European public administrations, businesses and citizens (ISA²) – Final study. Ed.: InformaticsG European Commission. Publications Office. Brussels.

Robles, J. M.; Torres-Albero, C.; Villarino, G. (2021): Inequalities in digital welfare take-up: lessons from e-government in Spain. In: *Policy Studies*, S. 1–16.

Syvertsen, T., Enli, G., Mjøs, O.J. and Moe, H. (2014): *The Media Welfare State*: Nordic Media in the Digital Era, University of Michigan Press.

TUM & Initiative D21 (2021): *eGovernment Monitor 2021*: Staatliche Digitalangebote - Nutzung und Akzeptanz in Deutschland, Österreich und der Schweiz. Ed.: Initiative D21 & Technische Universität München.

TUM & Initiative D21 (2022): eGovernment Monitor 2022. Nutzen und akzeptieren Bürger*innen die digitale Verwaltung? Die deutschen Bundesländer, Deutschland, Österreich und die Schweiz im Vergleich. Ed.: Initiative D21 & Technische Universität München.

UN (living document): Digital Inclusion. Digital Inclusion. Ed.: United Nations office of the secretary-general's envoy on technology. *United Nations (UN) (Roundtable on Digital Inclusion).* Online available: https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Definition_Digital-Inclusion.pdf, last checked 1st of Oct 2023.

Van Deursen, A.J.A.M. and Helsper, J.E. (2015): "The third-level digital divide: who benefits most from being online?", in Robinson, L., Cotten, S.R., Schulz, J., Hale, T.M. and Williams, A. (Eds), *Communication and Information Technologies Annual* (Studies in Media and Communications), Vol. 10, Emerald Group, Bingley, pp. 29-52.

Van Dijk, J. (2005): The Deepening Divide: Inequality in the Information Society. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc.

Wu, J. and Hayward, M. (2023): International impact of the GDPR felt five years on, Pinsent Masons, https://www.pinsentmasons.com/out-law/analysis/international-impact-of-the-gdpr-felt-five-years-on

Annex A

A.1 Results for 'number of OPS'

The table below shows three regression models in which we progressively introduced the socio-demographic variables (model 1), then new technologies (model 2) and digital skills (model 3) and finally welfare regimes (model 4).

	Dependent variable:			
	Number of OPS used			
	(1)	(2)	(3)	(4)
Age	0.001	0.01	0.02	0.03**
GenderMale	0.15	-0.09	-0.25	-0.28
EducationVocational	1.18	1.22	1.15	1.30*
EducationUniversity	1.14*	1.17*	0.87	1.45**
Income1	-0.97	-0.92	-0.76	-0.21
Income2	-0.69	-0.61	-0.42	-0.22
Income4	0.36	0.36	0.24	0.41
Income5	0.44	0.37	0.36	0.36
EthnicityMinority	-0.45	-0.37	-0.09	0.45
CitySmall	-0.12	-0.09	-0.10	0.01
CityMajor	0.62	0.63	0.61	0.49
CitizenshipResident	-0.23	-0.12	-0.26	-0.31
new Technology		0.51***	0.28	0.27
digitalSkillIndex			0.04***	0.03**
WRConservative				0.44
WREasterDemocratic				2.65***
WRSouthernDemocratic				2.23***
Constant	3.38***	1.20	-1.56	-3.18**
Observations	561	561	561	561
R^2	0.03	0.04	0.06	0.13
Adjusted R^2	0.01	0.02	0.03	0.10
Residual Std. Error	3.97 (df = 548)	3.95 (df = 547)	3.92 (df = 546)	3.78 (df = 543)
F Statistic	1.24 (df = 12; 548)	1.81** (df = 13; 547)	2.39*** (df = 14; 546)	4.72*** (df = 17; 543)
Note:				*p<0.1; **p<0.05; ***p<0.01

Figure 31 Regression models for 'number of OPS'

A.2 Results for 'usage of eGovernment services'

The table below shows three regression for the usage of eGovernment services models in which we progressively introduced socio-demographic variables (model 1), new technologies and digital skills (model 2) as well as welfare regimes (model 3).

results of all three models

	Dependent variable:		
	usage of eGovernment		
	(1)	(2)	(3)
Age	-0.02**	-0.01	0.01
GenderMale	0.25	-0.01	-0.02
EducationVocational	-1.14	-1.24	-1.21
EducationUniversity	-0.51	-0.79	0.02
Income1	-1.05*	-1.00*	-0.49
Income2	0.68	1.00	1.37
Income4	0.34	0.15	0.41
Income5	0.61	0.50	0.56
EthnicityMinority	-1.32**	-1.03	-0.45
CitySmall	0.21	0.21	0.43
CityMajor	0.61	0.56	0.54
CitizenshipResident	-0.77	-0.95	-1.18*
new Technology		0.16	0.26
digitalSkillIndex		0.04***	0.03**
WRSocialDemocatic			4.05***
WREasternEuropean			0.10
WRSoutherEuropean			2.59***
Constant	3.29***	-0.81	-3.12**
Observations	587	587	587
Log Likelihood	-168.96	-158.65	-126.29
Akaike Inf. Crit.	363.92	347.29	288.57
Note:	*p<0.1; **p<0.05; ***p<0.01		

Figure 32 Regression models for 'usage of eGovernment services'

A.3 Results for welfare regimes[29]

Another four regression models are shown in the table below. For each of the four welfare regimes, we measured all socio-demographic variables as well as new technologies and digital skills.

	Dependent variable:			
	Number of OPS used			
	eastern european	conservative	social democratic	southern european
	(1)	(2)	(3)	(4)
Age	0.01	0.03	0.02	0.05*
GenderMale	-0.39	-0.41	0.41	-0.64
EducationVocational	-1.09	0.64	2.05	0.78
EducationUniversity	-0.29	0.45	1.85	1.91*
Income1	0.32	-0.80	-0.79	-1.86
Income2	-0.06	-2.03	0.14	-0.65
Income4	1.51	0.36	-1.09	0.90
Income5	0.12	-0.79	-0.02	1.13
ÉthnicityMinority	0.07	1.64	-1.07	-0.51
CitySmall	-0.87	0.18	-0.69	0.15
CityMajor	-0.99	1.16	-0.80	0.75
CitizenshipResident	1.65	-0.67	-0.78	0.85
new Technology	-0.28	0.69*	-0.04	0.12
digitalSkillIndex	0.07**	0.03	0.04	0.04
Constant	-0.29	-3.13	1.21	-2.43
Observations	27	172	123	239
R^2	0.70	0.09	0.07	0.07
Adjusted R^2	0.34	0.005	-0.06	0.01
Residual Std. Error	1.42 (df = 12)	4.14 (df = 157)	3.85 (df = 108)	3.74 (df = 224)
F Statistic	1.96 (df = 14; 12)	1.06 (df = 14; 157)	0.54 (df = 14; 108)	1.23 (df = 14; 224)
Note:				*p<0.1; **p<0.05; ***p<0.01

Strongly significant Weakly significant

Figure 33 Regression models for 'welfare states and number of OPS'

[29] In all models, the conservative welfare state was set as the reference category.

A.4 Results for countries

The regression model has also included countries as variables into the usage of OPS per year.

	Dependent variable:
	Number of OPS used
Age	0.05***
GenderMale	-0.22
EducationVocational	0.86
EducationUniversity	1.06*
Income1	-0.02
Income2	-0.28
Income4	0.08
Income5	-0.06
EthnicityMinority	-0.55
CitySmall	0.15
CityMajor	0.97**
CitizenshipResident	0.13
Denmark	2.62***
Finnland	3.12***
France	5.42***
Germany	-0.97
Iceland	1.24
Italy	0.76
Spain	2.75***
new Technology	0.32*
digitalSkillIndex	0.03**
Constant	-3.34**
Observations	561
R^2	0.23
Adjusted R^2	0.20
Residual Std. Error	3.57 (df = 539)
F Statistic	7.57*** (df = 21; 539)
Note:	*p<0.1; **p<0.05; ***p<0.01

Figure 34 Regression model for countries

A.5 Results for IMPULSE[30]

The table below shows a regression for the approval of IMPULSE. It contains socio-demographic variables, new technologies and digital skills as well as welfare regimes as variables.

	Dependent variable:
	approval of IMPULSE
Age	0.0003
Gender-Male	-0.11
Education-Vocational	-0.18
Education-University	-0.13
Income1	0.06
Income2	0.51**
Income4	0.23
Income5	0.35**
Ethnicity-Minority	-0.16
City-Small	-0.11
City-Major	-0.02
Citizenship-Resident	-0.11
new Technology	0.25***
digitalSkillIndex	0.002
WR-Conservative	0.19
WR-EasterEuropean	1.21***
WR-SouthernEuropean	0.44***
Constant	1.96***
Observations	610
R^2	0.13
Adjusted R^2	0.10
Residual Std. Error	1.15 (df = 592)
F Statistic	4.99*** (df = 17; 592)
Note:	*p<0.1; **p<0.05; ***p<0.01

Figure 35 Regression model for the approval of IMPULSE

[30] The very low case number of "No" in the case of social democratic but also central and eastern European and southern European is a problem for the predictive power of the model.

A.6 Digital Skills Index

Weight¤	I know how to…¤
1¤	…use Google or other internet search engines¶ …use email or social media¶ …use Word or Powerpoint¤
2¤	…find relevant information and forms on websites of state agencies like ([*country-specific example, e.g. local government office, unemployment agency*])¶ …save or store files (documents, music, films etc.) on my device and retrieve them when I want them¤
3¤	…use Cloud Applications like Dropbox, iCloud, Google Drive, SharePoint to store and share documents¶ …use online services like e-banking, e-governments, e-hospitals etc.¶ …re-install or update computer programs¤
4¤	…read a simple computer code and make basic changes to it¤

Table 7 Digital Skill Index

A.7 Measuring digital needs

A.7.1 Control of data

1: Online service providers have to ask for my consent before collecting or using my data.

2: Online service providers must provide a short, easy-to-understand privacy policy explaining how they use my data.

3: Online service providers may not request more data from me than is necessary to provide the service.

4: Online service providers cannot refuse to provide their services just because I do not consent to their use of my information for advertising.

5: Online service providers cannot use website lay-out and other tricks that manipulate me to give them extra data or data-use permissions.

6: Online service providers must delete my data if I ask them to.

A.7.2 Preferred log-ins

1: User Name + Password

2: SmartCard + PIN-Number

3: PIN / TAN

4: Fingerprint recognition

5: Face recognition

6: Voice recognition

7: Eye [iris] recognition

8: Other [please specify]

A.7.3 Suggestions for improve

1: Make signing up for eGovernment (creating a digital identity to use for eGovernment) easier and faster

2: Make logging-in to eGovernment services easier and faster

3: Make more public services available online

4: Make finding information about eGovernment services easier

5: Improve the layout of eGovernment websites

6: Offer more assistance for using eGovernment (e.g. helplines, chatbots)

7: Ensure all eGovernment services can be completed fully online (i.e. no need for any offline steps, like providing physical signatures)

A.8 Interview guideline for expert consultations

Part 1: Digital inclusion in your country

- The research literature discusses digital inclusion with regard to: a) access to technologies, b) internet connectivity, c) digital skills, d) access to content, e) trust in digital technologies, f) social inclusion, g) access to public services.
- What does digital inclusion mean in your country? Which conditions particularly promote or hinder digital inclusion in your country?
- In your country, what are the main barriers of digital inclusion? Which social groups are most likely be affected by social exclusion?
- What is done to reduce the risks of digital exclusion? Which state or non-state actors are most engaged in tackling these risks?

Part 2: Impact of eID solutions on digital inclusion

- In your country, what does the introduction of novel eID solutions mean for digital inclusion?
- Which social groups would most likely be affected by social exclusion due to new eID solutions? Please name the most vulnerable groups and explain why those groups are affected?
- What are the main barriers of digital inclusion in particular with regard to accessing public online services?
- Which of these barriers apply for specific social groups? Please explain why?

Part 3: Policies or strategies of digital inclusion

- In your country, what is done to promote digital inclusion at the level of national government, country regions and/or cities? Please think of
  - Service providers
  - Implementation process
  - State policies and regulation
  - Other policies or measures
- Reflecting on the policies or measures just discussed, which of them would particularly apply for those social groups that were discussed in part 2 in order to promote their digital inclusion?

Part 4: Digital inclusion due to IMPULSE?

From the User's perspective, the key features of IMPULSE are thus

- biometric (facial) recognition instead of username/password or similar
- Arguably some increased level of control over their own data, due to
  - data storage on device
  - disintermediation of identity management providers (e.g. "log in with Facebook")
  - transparency over what data was disclosed to which service provider
- Do you consider the use of biometrics for registration/authentication instead of passwords/username, PINs etc. to have any meaningful inclusionary or exclusionary effects? For which social groups?
- Would ensuring that users have "control" over their own data have meaningful inclusionary effects?
- To what extent would you consider IMPULSE to in fact provide users with meaningful control over their data?
- Would you expect any other aspects of IMPULSE to have meaningful effects on inclusion/exclusion?