Identity Management in PUbLic SErvices

6.2 Background assessment and recommendations report

Lead Author: Bernd Beckert
With contributions from: Nicholas Martin, Furkan Cinar
Reviewer: Bertille Auvray, Syed Naqvi

Deliverable nature:	R
Dissemination level: (Confidentiality)	PU
Delivery date:	09-05-2023
Version:	1.0
Total number of pages:	249
Keywords:	Electronic Identity, e-government, e-business, ideation of new cases, requirements for introduction, country reports

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

Executive summary

This report summarizes the results of six expert workshops carried out between December 2022 and March 2023. The aim of the workshops was to present the IMPULSE project to a wider expert community in the countries involved in the project and to identify new use cases, possible application fields as well as to discuss critical issues that might emerge when adapting the IMPULSE system in the different countries. The six countries where the workshops were held were: Bulgaria, Spain, France, the Nordics (Denmark, Finland, and Iceland), Italy, and Germany.

This deliverable relates to Task 6.2 of the IMPULSE project, „Ideation of new fields of deployment and innovation“, which was coordinated by Fraunhofer ISI and supported by all project partners. The task comprised the identification of local experts, the organization of the online workshops, the realization of presentations in the respective national languages, and the documentation of the expert discussions. In addition, background reports were researched and written up which analyze the state of introduction and use of electronic ID systems in the six countries. The country reports provide indications of where the IMPULSE solution could link to in each of the selected countries or which existing systems it will encounter there.

The results of the workshops and background reports presented here contribute in the wider project context to the planned roadmaps and the routes to exploitation and sustainability of the IMPULSE solution. The main question to be answered in these project parts is how the IMPULSE solution or parts of the IMPULSE system could be used to extend or improve existing eID schemes in European countries.

This report has two parts: The summary part and the part containing the comprehensive documentation of the workshops. The summary part contains background assessments and a list concerning needs and demands in the different countries. And it contains a list of requirements for the further development of the IMPULSE solution. Both lists are of particular importance for the further discussion of measures concerning the dissemination (roadmaps) and sustainability (exploitation) of the IMPULSE solution.

The second part of this report (Annex A) contains the documentation of the six workshops and shows possible connecting points of the IMPULSE solution in more detail.

Overall, the report shows that the possibilities where IMPULSE could link into existing solutions in the different countries are not uniform, but very specific: In each country the eID situation is different which means that individual dissemination strategies have to be found for the IMPULSE solution.

Document information

Grant agreement No.	**101004459**	**Acronym**	**IMPULSE**
Full title	**Identity Management in PUbLic SErvices**		
Call	DT-TRANSFORMATIONS-02-2020		
Project URL	https://www.impulse-h2020.eu/		
EU project officer	Giorgio CONSTANTINO		

Deliverable	**Number**	D6.2	**Title**	Background assessment and recommendations report
Work package	**Number**	WP6	**Title**	Roadmapping for adoption, escalation, and sustainability
Task	**Number**	T6.2	**Title**	Ideation of new fields of deployment and innovation

Date of delivery	**Contractual**	M26	**Actual**	M27
Status	version 1		☐Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)	Bernd Beckert (Fraunhofer), Nicholas Martin (Fraunhofer), Furkan Cinar (Fraunhofer)			
Responsible author	**Name**	Bernd Beckert		
	Partner	Fraunhofer	**E-mail**	Bernd.Beckert@isi.fraunhofer.de

Summary (for dissemination)	Synthesis report based on six expert workshops in which the further use of the IMPULSE solution in the different county contexts was discussed. In addition, country reports on the current state of introduction and use of eIDs in the six countries are provided. Recommendations on the further development of IMPULSE are given.
Keywords	Electronic Identity, digital identity, e-government, e-business, ideation of new cases, requirements for introduction, country reports

Version Log

Issue Date	Rev. No.	Author	Change
08.05.2023	**0.1**	**Bernd Beckert**	First draft
08.05.2023	**0.2**	**Nicholas Martin**	Internal review, various minor corrections
09.05.2023	**0.3**	**Bertille Auvray**	Corrections of spelling and grammar, additions to the French country report, suggestions for further analysis
10.05.2023	**0.4**	**Syed Naqvi**	Spelling and grammar corrections, suggestions to correct references, suggestions to clarify “needs”, “demands” and “requirements”.
11.05.2023	**V1**	**Bernd Beckert**	Accepted suggested corrections and worked in terminology suggestions, style checking with Grammarly of the summary part, adding additional info to the French country report.
22.05.2023	**V1.1**	**Bernd Beckert/** Nicholas Martin/ Alicia Jimenez	Final document formating

Table of contents

List of figures

List of tables

Abbreviations and acronyms

CQES	Cloud-Qualified Electronic Signature
DESI	Digital Economy and Society Index
EC	European Commission
eID	Electronic Identity
eIDAS	electronic Identification, Authentication, and trust Services
EU	European Union
NIST	National Institute of Standards and Technology
PA	Public Administration
QES	Qualified Electronic Signature
SSI	Self-Sovereign Identity
VC	Verifiable Credential
ZKP	Zero Knowledge Proof

1 Introduction

As an input to the roadmapping for adoption, escalation and sustainability of the eID solution developed in the IMPULSE project (WP6), strategic sessions were planned with external stakeholders. In these strategic sessions, new fields of deployment and innovation were to be identified (Task 6.2, see IMPULSE project description, p. 56).

Between December 2022 and March 2023, six strategic sessions were carried out as expert workshops in Bulgaria, Spain, France, Italy, Germany and the three Nordic countries Denmark, Finland and Iceland. This report documents the results of the workshops, provides additional background information on the state of the introduction of eID schemes in the six countries and gives recommendations for the further development of the IMPULSE solution.

Fraunhofer ISI coordinated the preparation and implementation of the workshops. The workshops were then carried out and documented by the local IMPULSE partners.

The workshops had two aims:

- firstly, in the workshops, the IMPULSE solution was to be presented and promoted to a larger group of experts in the participating countries, and
- secondly, the workshops should explore new possible use cases and docking opportunities with existing national or local eID solutions.

The target groups for the workshops were:

- DIH networks
- Public sector officials from various levels (local to national, potentially EU)
- Private sector service providers (verifiers/relying parties), e.g. banks
- Trust service providers
- eID vendors and other IT components suppliers
- Civil society
- Academic specialists (e.g. NIIS, OECD Blockchain Advisory, eIDAS observatory)

The workshops were organized as 1 to 1,5 hrs online workshops consisting of a presentation part and an interactive part. Table 1 shows the agenda of the Spanish workshop as an example.

The structure of the workshops was always the same, in the interactive part of the workshops there were minor deviations in the Bulgarian and Italian workshops, where there were no working groups, but discussions were held in plenary, and in the Nordic workshop where the break-out sessions were arranged in such a way that there was a Danish group and an Icelandic/Finnish group. The coverage of topics "Use cases", "Technical aspects" and "Regulation and Standards" was ensured to in all workshops, so that these variations had no influence on the uniformity of the results.

The actual implementation of the agenda, the distribution of participants among the stakeholder groups and the documentation of the discussions of the workshops can be found in the respective workshop documentation in Annex A. Annex B includes the presentation slides used by IMPULSE project partners to present the IMPULSE solution in the different languages.

TIME	ACTIVITY
10 minutes before the start	Arrival of participants
Keynotes	
10:00-10:10	Overview of the IMPULSE-solution, including use cases: Javier Gutiérrez Meana (TREE), Jiri Musto (LUT) or Nicholas Martin (Fraunhofer ISI)
10:10-10:20	Technical aspects and questions: Jaime Loureiro (Gradiant)
Participatory Breakout Sessions	
10:20-11:00 (participants can select which session they want to join)	Session 1: Use cases (Spanish)
	Session 2: Technology aspects (Spanish)
	Session 3: Regulation & standards, ethics, politics and law (English)
Optional: Wrap-up	
11:00-11:10	Summary and final remaks

Figure 1 Agenda of the Spanish Workshop showing the general structure of the workshops

Source: www.isi.fraunhofer.de/en/veranstaltungen/2023/eu-impulse-smartphone-based-digital-identities-facial-recognition-spain.html

Table 1 shows the number of experts participating in the different workshops, altogether 125 external experts have actively participated.

Country	Number of external participants	Date of the workshop
Bulgaria	8	December 14, 2022
Spain	20	January 26, 2023
France	14	February 23, 2023
Nordics (Denmark, Iceland, Finland)	24	March 2, 2023
Italy	41	March 14, 2023
Germany	18	March 30, 2023

Table 1 Workshops carried out in the six countries with number of participants and date

This report is structured as follows: In the following section (section 2), we will provide an overview of the eID situation in the six countries. The basis for this overview table are the so called background reports which were prepared by Fraunhofer ISI for each country and which are documented in full in Annex A. Section 3 then contains the main results and recommendations compiled from the workshops. The recommendations are structured in two parts: Firstly, „Needs and demands“ summarise the suggested use cases in the different countries and lists the specific aspects, participants highlighted in the workshops. Secondly, „Requirements“ summarises what workshops participants suggested as further developments of the IMPULSE solution. Section 4 contains our conclusions and an outlook including next steps for the IMPULSE-team.

2 Background assessment: The state of introduction of eIDs in the six participating countries

Based on the insights of the background reports analysing the introduction and use of eID schemes in the six countries, table 2 shows which systems are in use in mid-2023 in which application domains (e-government, banks and other businesses, health).

Country	e-Government	Online banking and e-business	e-Health	Remarks
Bulgaria	planned	Evotrust B-Trust	no info	IMPULSE Pilot in Peshtera
Spain	DNIe 4.0/ DNIe en el móvil, Gijon Citizens Card, Cl@ve, regional systems (Tarjeta Ciudadana or idCAT Mòbil)	different systems	Cl@ve, regional apps (Meva Salut app in Catalunya)	IMPULSE Pilots in Gijon and the Basque Country
France	FranceConnect +, CNIe/ SGIN	La Poste eID, Mobile Connect by Orange, different e-banking systems	Ameli (health insurance online)	Facial recognition system ALICEM stopped in 2022
Denmark	MitID/ MitID app (used to be NemID until June 2023) Sundhed.dk			IMPULSE Pilot in Aarhus
Finland	Finnish Trust Network (FTN) (used to be Tupas until 2019), FINeID Kela´s MyKanta			-
Iceland	Ísland.is eID Heilsuvera			IMPULSE Pilot in Reykjavik
Italy	CIE/ CieID app, SPID	different systems	not planned	IMPULSE Pilot with InfoCamere
Germany	Ausweisapp 2 eID, BundID	different systems	not planned	Highly controversial pilots for facial recognition for law enforcement

Table 2 Available eIDs in six European countries

Concerning the actual use of eIDs in the selected countries, we can find four different groups, as table 3 shows. Group 1 are the Nordic countries where eID use is between 80 and 90 percent in the population. Group two is made up of Spain where there is a low usage of the national eID systems DNIe or Cl@ve but where certain regions or even localities have their own eID systems, often in form of Citizen Cards, which have a high usage of over 40% (even higher in some municipalities). The third group are countries with existing eID systems which have a low usage, France, Italy and Germany. The fourth group consists of Bulgaria, where a national eID solution has yet to be implemented and the private schemes have a low usage.

Country	Use of eIDs in the population (estimates)	Group
Nordics (Denmark, Iceland, Finland)	80-90%	1
Spain	over 40% in certain regions with local eID schemes, national eID use is below 10%	2
France	below 10%	3
Italy		
Germany		
Bulgaria	in early stage	4

Table 3 Use of eIDs in selected countries in 2023

Source: Own compilation based on the country reports, see Annex A

These findings are supported by research for example by consulting firm Oliver Wyman (2021). In their report „Digital Trust. How banks can secure our digital identity" three different levels are used to characterize eID penetration in European countries: „Mature" with more than 40% of the population using eID systems, „Active" with a penetration rate below 5% and „No eID scheme". According to their overview, the Nordics have „Mature" eID-markets; Spain, France, Italy and Germany have „Active" eID-markets; and Bulgaria has „No eID scheme".

It has to be noted that „owning" an eID especially in the middle group sometimes is very different from actually „using" it. With passports and state identity cards increasingly having eID functionality, growing numbers of European citizens actually own an eID because it is automatically part of their ID card. However, to use it, citizens need to register online which usually implies that they have received a letter with their PIN from the public administration or to register via other credentials like tax signatures. In 2023, the mobile use of eIDs based on national IDs for authentication is still in its beginnings although progress into this direction can clearly be seen.

2.1 E-government maturity of European public administrations

The fact that we are dealing with three groups of countries in our country selection is confirmed when we look at the results of the e-government ranking. The availability of public administration services that can be completed digitally is one of the prerequisites for eID use in the population. To assess the e-government services availability of our countries, the Digital Economy and Society Index (DESI) of the European Commission can be used.

The DESI digital public services ranking is based on an indicator that measures the extent to which a service or information of the public administration is provided online. The indicator represents the share of steps that can be done online for major life events. The indicator balances the importance of the different services provided at the national level (see DESI 2022, p. 6). The rating is provided for citizen services (table 4) and for services the public administration offers for businesses (table 5). The rating is available for 27 EU countries but does not include Iceland.

Three clusters emerge when analysing the ranks for our selection of countries (excluding Iceland):

Group 1 with a mature e-gov infrastructure (Denmark, Finland, Spain), group 2 with a medium level of e-gov availability (France, Germany) and group 3 with a lower level of e-gov-services (Italy, Bulgaria).

Own clustering	Country	DESI-Ranking
1	Finland	4
	Spain	6
	Denmark	9
2	Germany	14
	France	18
3	Italy	21
	Bulgaria	24

Table 4 Digital public services for citizens according to DESI 2022

Source: DESI 2022, p. 6 (Iceland is not included in DESI analysis)

Own clustering	Country	DESI-Ranking
1	Spain	5
	Finland	7
	Denmark	8
2	France	18
	Germany	19
3	Italy	20
	Bulgaria	21

Table 5 Digital public services for businesses according to DESI 2022

Source: DESI 2022, p. 7 (Iceland is not included in DESI analysis)

A different source to assess the e-Gov maturity is the „eGovernment Benchmark“ report, carried out by Capgemini for the European Commission (eGovernment Benchmark 2022, Insight Report). Their study includes Iceland. The eGovernment Benchmark is also a composite indicator but has a slightly different weighting. It includes score averages in the thematic areas of user centricity, transparency, key enablers and cross-border services. According to this analysis, a similar picture arises with Iceland leading the top group, Spain and France in the medium group and the three countries Germany, Bulgaria and Italy in the lower group (table 6).

Own clustering	Country	e-Gov Benchmark-Ranking
1	Iceland	2
	Finland	6
	Denmark	7
2	Spain	11
	France	18
3	Germany	21
	Bulgaria	23
	Italy	24

Table 6 Country overall e-Government Benchmark maturity

Source: eGovernment Benchmark 2022, Insight Report, p. 16.

Concerning e-government services in European countries, the study also found that out of those public administration services that require identification, 21% still require users to show up personally in an office and present their identity card (see figure 1). 67% of the administrative services that require identification allow for online identification with an official national eID. 11% of the services required logins via other online government mechanisms (e.g. organisation-specific account and password, national registration or tax number), and 1% allow private sector mechanisms (e.g. eBanking token).

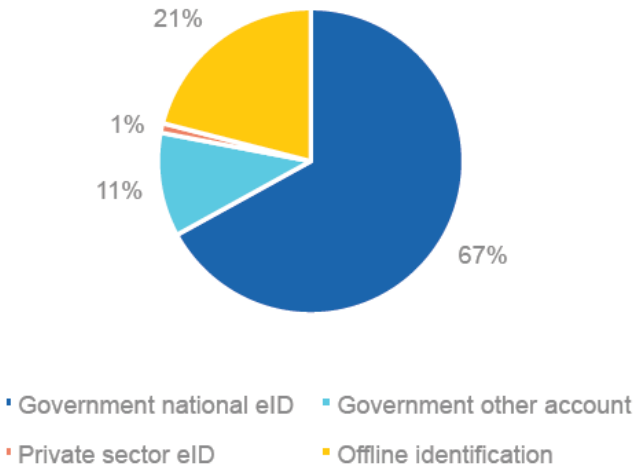


Figure 2 Percentage of identification modes EU27

Source: eGovernment Benchmark 2022, Insight Report, p. 2.

The eGovernment Benchmark report identifies Iceland, Denmark, Estonia, Finland, Norway, Malta and Lithuania as „Europe's eID frontrunners, where more than 90% of the services can be accessed using the national eID" (eGovernment Benchmark 2022, p. 2).

3 Recommendations: Needs, demands and requirements concerning the IMPULSE solution

In this section, the results of the six workshops are summarized according to the dimensions „Needs and demands“ and „Requirements for the further development of the IMPULSE solution“. The information provided in this section originates entirely from the workshop. Details and explanations can be found in the documentation of the workshops in Annex A.

3.1 Needs and demands

Table 7 lists the most relevant contributions of the participants of the six workshops concerning „Needs“ and „Demands“. The following specifications were made:

- **“Needs”**: In the workshops we have asked participants which use cases they see for the IMPULSE solution in their country. The first column in table 7 thus lists the application contexts for which participants said that the IMPULSE solution may be “needed” in their country. In the German workshop there was a discussion as to whether there are any use cases at all for eID systems. One participant argued that since there is no willingness to pay for eIDs, we cannot speak of “use cases” in the conventional way. Others disagreed saying that as soon as eID systems become more user friendly, use cases will automatically develop. In the other workshops, possible use cases mentioned were, among others, “customer onboarding”, “extension of existing eID for disabled persons or expats”, “integration into regional eID systems for better usability”

- **“Demands”**: We have also asked participants in the workshops which aspects they considered to be the most pressing or relevant when introducing eID systems or using existing eID systems in their country. In table 7, the participants' remarks were summarized in keywords in the right column. The word „Demands“ thus is not used in the usual sense but in the sense of “what are the demands of the times when it comes to introducing eIDs or when trying to improve their usability in those countries where eIDs are are already widely used. The right column in table 7 also gives an account of what was being said concerning the general context of the eID situation in the respective country. Thus, in the “Demands”-column more general remarks, characterizing the current country-specific discussion can be found as well.

Country	Possible use cases for the IMPULSE solution („Needs“)	Most relevant issues concerning the introduction and use of eIDs („Demands“)
Bulgaria	Onboarding of customers of banks and insurances. E-gov-services are available, back-office digitization is on track, but a national eID scheme is yet to be implemented and bank eIDs rarely used.	Combine technical and legal aspects is a complex task. Political instability as a barrier. Safety, fraud prevention, privacy are key issues in Bulgaria. Business use and e-gov shall be combined. Legal aspects of eIDs are currently most pressing. Usability of the system is key.

Spain	Integration into existing regional and municipal eID projects. E-gov as well as payment functions are of interest.	Usability of the identification process. Time it takes for the user to get his/her eID registration done. Co-existing or replacing current eID-projects? Blockchain and DLT: What do users need to know about it? Implementation of EU regulation will take until 2027! Currently no certification scheme for remote biometric enrollment.
France	E-gov services especially for rural areas wanted. E-voting/ e-participation/ e-complaints. Access to welfare services for citizens in fragile situations. Notary offices in rural areas could serve as eID facilitators, especially for the elderly using e-gov services.	Fear of surveillance and abuse of personal/ biometric info: „Controlling of the population!“ Digital literacy of the population and confidence in e-solutions is a problem. High level of security is needed because of cyberattacks. Trust is given to banks and telco operators. Usability is key.
Denmark	User onboarding of persons, not being citizens of the Nordics (having no central personal number). How will a common EU eID look like? Will European eIDs be compatible with each other? Facial recognition helps the disabled in the onboarding process. User onboarding without having to show up in person. Integrate e-health and share health data in then system.	Manual ID-checks are required by EU law will be a problem when scaling up. Secure against cyberattacks. Security of the system is key. Does it make sense to have multiple eIDs for the users or does it confuse users? (in the analogue world, we have ID cards, passports, driver´s licences, etc.) Trust in the eID system is key User-friendliness is important.
Iceland, Finland	Moving from password-based to eID systems. Disabled citizens using facial recognition eID systems. Foreigners and expats need to use national eID systems but are not able to. Maybe IMPULSE can help. How to set up a unique unifier (as the Nordics have) in Europe?	Integrate people into the system who are foreigners and have no country registration. Are existing eID systems compatible with eIDAS and other European regulations? Will they become obsolete is there will be an EU-solution? Ease of use, simplifications for a more inclusive eID system and its services. From Nordic´s experience, it takes time to build up an eID-infrastructure. Not only technical aspects are important but clients, standards and rules. Path dependencies: New system will be difficult to establish when there are already working ones. Esp. service providers will be reluctant. Technology changes very fast, regulative audits have to be repeated often.

Italy	E-gov-services for citizens and businesses To be used as a general ID means granting access to the workplace, the gym, etc.	User-friendliness makes eID systems more attractive. Italians are familiar with the use of eIDs (SPID system). Difficulties to establish a second eID system like IMPULSE when people are already familiar with one. Privacy and security of data stored.
Germany	E-gov-services lagging behind. No willingness to pay: Frequent use cases are trivial and don´t need high security level (railway ticket) and use cases which require high security level are rare. Higher usability like in the IMPULSE solution will increase number of use cases and users.	Higher level of security is needed in Germany than elsewhere. Government needs to take the lead. Usability of eID solutions is very important. SSI-solutions have many advantages. Privacy concerns are central. One single eID or many different with different levels of assurance? Usability of the system is very important.

Table 7 Main results from the workshops: Needs and demands

Security and usability of the eID system are common demands in all countries. Here, the usability of the IMPULSE solution is highlighted and seen as an opportunity for higher penetration of eIDs and a more inclusive use. Concerning the security aspect, critical questions were being asked concerning the IMPULSE solution.

3.2 Requirements for the further development of the IMPULSE solution

Asked specifically which requirements participants of the workshops see in relation to the IMPULSE solution, a variety of aspects were mentioned. Table 8 summarizes the most important questions. Again, details are documented in the respective workshop documentation in Annex A. We use the following definition:

- **"Requirements":** In the workshops, we were interested to hear from participants how they assess the IMPULSE solution from their expert point of view. We asked very concrete questions like: "Which technical requirements does the IMPULSE solution need to fulfil in order to be implemented in existing systems?", or "Which aspects do we need to consider in the further development of the IMPULSE solution to make it applicable in the respective country?".

The table is a first compilation of requirements and questions and includes the most important aspects from the discussions. In a second step, which is planned in the following tasks of WP6, a systematic analysis of the mentioned requirements is necessary.

Country	Requirements for the further development of the IMPULSE solution
Bulgaria	▪ How to ensure the official, binding character of the IMPULSE solution in e-gov and e-business contexts? ▪ Make clear that the IMPULSE solution is a technical system and not an identity provider.
Spain	▪ What are the advantages of the video ident solution in IMPULSE which still needs an official person to verify, compared to other video ident solutions in Spain? ▪ Which technical controls can be introduced to replace the official person verifying the information in the IMPULSE enrolment process?

	▪ Explain and communicate the advantages of DLT compared to centralized systems to decision makers and users.
France	▪ How is the IMPULSE solution secured against deep fakes? ▪ How long are ID-videos of users stored on the server? ▪ How to deal with company eIDs? Are there company eIDs in IMPULSE? People do not want to sign in their own names for company affairs. ▪ What is being done against cyberattacks? ▪ Who is responsible in case of fraud in the IMPULSE-system? ▪ How does IMPULSE deal with false identification/ false rejection? ▪ Procedure to follow after the death of a person.
Denmark	▪ Can IMPULSE read the formats of ID cards issued outside the EU? ▪ How to deal with deep fake technology? ▪ How to minimize false negatives when faces of people are changing over time? ▪ How to deal with cyberattacks?
Iceland, Finland	▪ There are uneven eID-landscapes in Europe: IMPULSE needs to decide what shall be a priority: Develop a widely used solution for e-gov and e-business in beginners countries or focus on advanced countries which mainly ask for interoperability and add-ons for their existing systems. ▪ Do not only consider technical aspects but questions of liability, compliance, business responsibility in case of fraud. ▪ The auditing process of implementation takes a lot of time. ▪ How does IMPULSE relate to the EU eWallet-initiative and also to the Large Scale Projects? ▪ Interoperability: What is the process if other interlinked systems change features? ▪ IMPULSE competes against systems that use NFC capabilities of national ID cards which are much more secure. ▪ Maturity of IMPULSE needs to be reached before it can complement Nordics´ eID systems.
Italy	▪ Make clear where exactly personal data is stored and how it is secured and who can access it besides the owner. ▪ How can IMPULSE contribute to the eWallet-implementation? ▪ What is the difference between the eID of IMPULSE and the certificates used to sign documents?
Germany	▪ Check selfie-ID-process to be replaced by face-ID of mobile devices („trusted execution environment“) ▪ Do tests to ensure „substantial“ level of assurance is really achieved. ▪ Use of the image data stored on the German ID card for verification? ▪ Which protocols and formats are used in IMPULSE? How is interoperability with other solutions technically addressed?

Table 8 Summary of the future requirements for IMPULSE according to workshop experts

The questions asked with specific relation to the IMPULSE solution can support the process of drafting a roadmap for the further development of IMPULSE. In addition, the aspects mentioned here can be starting points for discussions on the exploitation of the IMPULSE project.

Recurring requirements and questions in table 8 are:

- Manual verification instead of fully automatic onboarding.

- How to avoid false negatives/ positives?
- How to secure against cyberattacks?
- eWallet initiative of the EU: How does IMPULSE relate to it?

The observation that in Europe there are three different levels of eID-implementation and use (Nordics with their mature eID market, Bulgaria having just started to develop their own eID system and the other countries in between having some eID usage and a sometimes fragmented eID market) poses the strategic question concerning the exploitation of IMPULSE: Shall the team focus on developing a widely used solution for e-gov and e-business in beginners and medium-use-countries or focus on advanced countries which implies to focus on interoperability aspects and ease of use.

4 Conclusions and Outlook

Based on the results of six country workshops, this report summarized the needs and demands concerning eID solutions in the different countries as well as requirements for the further development of the IMPULSE solution in order to link to existing solutions. The results of this analysis will feed into the activities of the IMPULSE project to disseminate and exploit the IMPULSE solution in the course of the project and to indicate possible directions after the official end of the project.

The report summarized the needs and demands in the different countries concerning eID solutions against the specific backgrounds of their introduction and use. It became clear that there is a wide range of possible further use cases for the IMPULSE solution in the various countries. The suggestions ranged from onboarding for online-banking to helping disabled citizens to log in, to notary services in rural areas. Concerning demands, the experts highlighted the need for usability, the combination of business use and e-government and the need for a high level of security.

Usability and security of the eID system were the most important demands in all countries. Here, the usability of the IMPULSE solution was highlighted and seen as an opportunity for higher penetration of eIDs and a more inclusive use. Concerning the security aspect, a number of questions were raised concerning the IMPULSE solution.

Of particular relevance for the further development of the IMPULSE solution is the list of aspects, experts considered critical for a possible introduction of IMPULSE in their respective country (table 9). Here, technical questions as well as strategic questions were asked. For example, it was suggested to carry out concrete technical tests to assure that the IMPULSE solution reaches the „substantial“ level. Another contribution focused on the strategic decision to either concentrate dissemination activities to countries where eIDs are just at a beginner´s level or on countries with already mature eID markets. As important as this list is, no prioritizations have been made yet.

The results of this report will feed into the further discussions of measures concerning the dissemination (roadmaps) and exploitation of the IMPULSE solution. Concerning concrete next steps, the roadmapping process can be mentioned first: Analysis provided in this report will directly feed into the roadmapping process in which the opportunities for a continuation of the pilots will be discussed.

Also, the results of this report will feed into the exploitation activities of the IMPULSE project (WP7).

A joint meeting of the roadmapping and exploitation teams to discuss the results of the workshops and the analysis presented in this report is foreseen as a concrete next step in the near future (mid 2023).

References

- DESI (2022): Digital Economy and Society Index (DESI) 2022. Digital public services. DG Connect, Brussels: European Commission, https://digital-strategy.ec.europa.eu/en/policies/desi
- eGovernment Benchmarking (2022): Background Report by Capgemini et al. July, DG Connect, Brussels: European Commission.
- eGovernment Benchmarking (2022): Insight Report by Capgemini et al. July, DG Connect, Brussels: European Commission.
- eID User Community (2023): Overview of pre-notified and notified eID schemes under eIDAS. Created by Marina Kirova and Dietmar Gattwinkel on Jan 24, 2023, https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
- European Commission; Deloitte (2021): Overview of Member States' eID strategies. CEF eID SMO Version 3.0, January 2021. Authors: Massimo Pedroli, George O'Neill, Arianna Fravolini et al.
- Pöhn, Daniela; Grabatin, Michael; Hommel, Wolfgang (2021): eID and Self-Sovereign Identity Usage: An Overview. In: Electronics 2021, 10 (22), 2811.
- Oliver Wyman (2021): Digital Trust. How banks can secure our digital identity. Report by consulting firm Oliver Wyman and the International Banking Federation (ibfed). Authors: Lisa Quest, Hang Qian, Simon Low et al. https://www.oliverwyman.com/our-expertise/insights/2021/dec/how-banks-can-secure-our-digital-identity-ibfed.html

Annex A Documentation of the six workshops

A.1 Documentation of the Bulgarian workshop on December 14, 2022

Title of the workshop:

Smartphone based digital identities using facial recognition for public services in Bulgaria. Presentation of the EU-"IMPULSE"-solution and discussion of use cases and requirements for adopting digital ID solutions in Bulgaria.

Who was in the workshop?

Host of the Bulgarian workshop was Georgi Simeonov from the Municipality of Peshtera. He and Nicholas Martin from Fraunhofer ISI had identified and invited a group of Bulgarian experts which were invited personally or via e-mail. The language of the workshop was English, so the selection of experts was limited to Bulgarians with English language skills. The invited experts were asked to register at the workshop webpage. The workshop was held online.

Nine external experts joined the workshop on December 14, 2022. From the IMPULSE project team, 19 persons joined the workshop. Since the Bulgarian workshop was the first in a series of six workshops to be held in the different partner-countries, there was great interest by the project members.

Agenda of the workshop

The 1h-online workshop had the following agenda:

- Presentation of the IMPULSE project including the presentation of the Peshtera pilot and its implementation challenges by Nicholas Martin from Fraunhofer ISI (15 min)
- Questions and answers concerning IMPULSE (5 min)
- Introductory round (5 min.)
- Discussion: Possibilities and constraints for adoption in Bulgaria (use cases, law & regulation and technology) using a prepared "Concept Board"-online tool where participants could write down their contributions before discussing them (30 min)
- Summary and next steps (5 min.)

The slides used for the presentation by Nicholas Martin can be found in the annex.

Documentation of the Q&A session

After the presentation of the IMPULSE project, its approach and technology used as well as the Pesthera use case, the following questions were asked by the participants of the workshop:

Q: The IMPULSE solution is developed for Android smart phones. Do you plan to make it available for iPhones as well?

A: Technically, it is also possible to make the IMPULSE solution available for iPhones, however, in the course of the project it is currently not planned.

Q: Could the presentation of the IMPULSE solution be made available for students of the University of Sofia? They might be interested in this interesting project and learn from the IMPULSE-approach and its insights.

A: The slides can be made available to the students. Also a video-clip of the presentation of Nicholas Martin can be taken. Another option is that experts from the IMPULSE project will visit the University of Sofia and do a presentation of the project in person. The University of Sofia offers to collaborate with the IMPULSE-team in further activities, for example when it comes to making the solution available for iPhone. A few slides would be enough to make students aware of the IMPULSE project and generate interest for blockchain

solutions in general. The Municipality of Pesthera proposes to involve interested students from the University of Sofia in a next phase for example when it comes to testing the implemented application.

Q: What is the ultimate goal of the project? What role will IMPULSE play in two or five years from now? Who shall use the IMPULSE solution? Will it be only for e-government services or for private companies as well? Who decides whether the IMPULSE solution will be used, government institutions or municipalities? Will the IMPULSE solution be officially recognized by the EU or which level of formalization do you aim for?

A: IMPULSE is a research project, it does not have a commercial motivation. But the solution we develop is a real-life solution which may actually be used in the future. In principle, the aim is that solutions like the one we propose in IMPULSE are widely used in Europe.

However, the work we do in the context of this project is preliminary, we will bring the solution to a technology readiness level (TRL) of 6. While for going to the market this would require a TRL of 9. So there are some steps of improvements and enhancements between our final project output and a market solution. We will address what it needs for this step after the end of the project.

The objective of the IMPULSE project is to develop and evaluate an eID solution which is based on AI –based facial recognition and blockchain. Since this is a radically new approach, we need to have assessments from different points of view before we can really say what is needed for a final implementation. To assess the practicalities of such an implementation, we have the pilots in the project in which different public administrations are involved. In the end, we will develop a roadmap for scaling up the the solution and also for engaging public administrations.

Documentation of the interactive part and discussion

Use cases

Concerning use cases, Bulgarian banks - like financial institutions elsewhere - are interested in solutions like IMPULSE because it enables the remote onboarding of customers. New customers do not have to come physically to the bank but can be authenticated via the online system. The bank can keep track of the new arrivals and can offer faster service with no waiting time and paperwork.

However, in practice, the implementation is very difficult. This concerns the user experience, the technical obstacles and in particular the legal part of the solution, including data protection. These three aspects are very challenging.

One participant from a large Bulgarian bank reports that they have reviewed several solutions offered by software companies providing services for digital identification. They have familiarised themselves with the subject and now wanted to find out about the IMPULSE solution.

The IMPULSE project team supported the finding that implementing such a system is a complex task. It was reported from the Pesthera use case that the originally planned fully-working pilot had to be scaled down because of technical and legal issues. It was still possible for test persons to play around with the system and give feed-back on the user experience, however, the system had no official or legally binding character. In this sense, the Pesthera pilot was a dry swimming exercise which gained valuable feed-backs about the user interface, but which did not change the paper-based process of issuing certificates of legal permanent address (see background paper on the situation of eID and digital signature systems in Bulgaria in the annex).

The experts in the workshop said that the discussion shall not be restricted to public administration use cases. Instead, private sector use cases, especially banking and financial services shall be targeted. Private services are more often used than public administration services. Private sector use cases give a citizens an incentive to actually install a system, they will be unlikely to do so if it is just public sector because there are too few occasions when they are needed.

Technology

Concerning technology aspects it was asked how the identification process actually works in IMPULSE and whether IMPULSE acts as an official identity provider. The question referred to the user registration and authentication process presented at the beginning of the workshop (see figure 1).

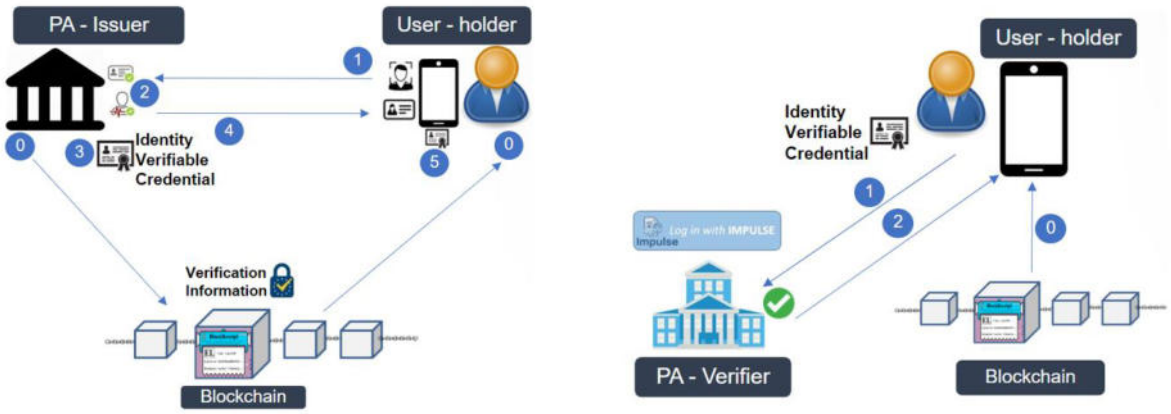


Figure 3 User registration and authentication via the IMPULSE system

Source: Nicholas Martin´s presentation at the workshop on December 14, 2022. PA: Public Administration.

The PA-Issuer and the PA-Verifier have to be service providers which are officially registered as identity providers. There are strict regulations in place for who can actually be such an identity provider. For any company offering a complete online authentication service, it is necessary to have an official recognition by a public organization or public agency that they are allowed to do this kind of authentication.

It was reported from an expert working in a Bulgarian bank, that it is a key requirement in Bulgaria that the organization which provides the service for identification must be a officially recognized by a public body. The question arising from this was whether the IMPULSE system acts as an official identity provider or intents to do this in the future.

The answer to this question was that IMPULSE is a research project and that IMPULSE does not act as a certified authentication issuer or verifier. In fact, an identity provider is a supplier of a trust service inside a electronic digital identity system. And in the IMPULSE project, we are not creating a trust system but a new technology for such a system. Even if the IMPULSE project may become a commercial project in the future, we will not become an identity provider.

In Bulgaria, two trust service providers exist which basically provide electronic signatures and electronic stamps (see annex “Background paper”). The Bulgarian experts from the banking sector said that they are already using the available systems in cases for digital customer onboarding, for signing documents electronically or in the payment service area. But only in a limited fashion, in an early stage of adoption.

The system they currently use works with one-time passwords which are generated in order to make electronic payments and to confirm your electronic identity when paying online with the credit card or via the bank account.

Law and Regulation

Asked about the main barriers for implementing eID solutions, participants of the workshop said that it is the legal side of the system that poses the highest barriers. From the organization´s perspective, the main show stopper is that every such technical solution has to comply with a large amount of legal requirements.

Whenever a technical solution in the payment service area is used, it must comply with the PSD tool currently used in the area of customer onboarding. Also, the system has to comply with requirements of the AML regulation before the institution or company can act as a qualified trust service provider.

From the viewpoint of customers, the solution has to be easy to use, it must be possible to install it on the home computer. It should require very few steps to register and users should be able to use it without the need to call the technical support or to write emails.

The experts emphasized the role of trust in the adoption process: The greatest attention must be paid to safety and the exclusion of fraud and fake identification. If the system cannot guarantee this, institutions and clients will not use the system.

In Bulgaria, people are very critical to digital systems in general. So the adoption of eID systems in Bulgaria depends on the ability to create trust in them.

Currently, for many people, eID systems seem very complicated, something they don't fully understand. So they may say, it is too complicated, I will not take the time to try to understand it, I don't trust it and therefore I will not use it.

General impression of the workshop

The workshop informed the expert community in Bulgaria about the IMPULSE project and presented the solution that is being developed in the project. It contributed to networking and allowed us to clarify important questions. The workshop was also important for the roadmap, but not all questions could be answered.

We have learned a lot about the needs of banks and we now know the conditions and difficulties of implementation in public administrations. But there is a lack of information about the other potential application areas.

The Bulgarian workshop was the first workshop of a total of six dissemination workshops. The decision to hold the Bulgaria workshop in English has limited the selection of experts and proved to be a barrier during the workshop. For future workshops, consideration should be given to holding them in the respective national language.

Overall, the planned duration of the workshop of one hour seemed too short. In future workshops, it should be considered to extend the workshop to 1.5 hours. Then there would also be more time to collect ideas with the help of the online tool "Concept Board".

After the workshop, an e-mail-Interview was carried out with the former Bulgarian Minister for e-Government. In addition, two further Bulgarian experts were asked for their assessments. The collected information has been incorporated into the background report.

Bulgaria: Background report

In 2023, there is no government-issued eID system in place in Bulgaria, although it has been planned for since 2006. However, there are two private eID and digital signature providers: B-Trust and Evotrust.

- B-Trust is a qualified digital signature system provided by the Sofia-based company Borca. For identification purposes, the company asks for a personal visit in one of their offices or use a videoident procedure for the mobile app. The B-Trust system can be used for online banking, tax declarations, and documents to be submitted to state and municipal authorities. The PC-version of the digital signature provided by BT-Trust is usually stored on the user´s PC. For persons who want to use electronic signature on multiple computers, the company offers a smart card and a card reader. The e-signature service (without smartcard and reader) is priced at 3 Euros per year or 8 Euros for three years. In addition, there is a initial registration fee of 3 Euros.

Physically, the B-Trust eID/digital signature system takes the form of a USB-Stick, which is password-protected, and a software package, which needs to be downloaded from the BTrust Website to the desktop computer. For mobile use, B-Trust offers the “B-Trust Mobile App”, which provides a cloud-qualified electronic signature (CQES). For registration, videoident is used. Three signings per year are free of charge, then the company charges a small fee per signature. The company says its “B-Trust Mobile App” is eIDAS compatible.[1] There is no information about the number of banks or companies which allow B-Trust identification for their services and no information about the number of users. B-Trust seems to be more widely used as Evotrust, however, the level of usage in the population seems lower than 5 percent (estimation of expert interviewed).

[1] https://www.b-trust.bg/en/electronic-signatures/products/cloud-certificates/cloud-standart

- Evrotrust provides similar solutions and has the same target groups, namely persons who what to use online banking, online payment, digital tax refund, application for state aid (esp. Corona aids), and turning in or signing documents to be submitted to state and municipal authorities. Evotrust relies entirely on the mobile videoident process for the identification of its customers. Five Evotrust e-signature s are free of charge, then a small fee is charged for every e-signature. Companies or authorities providing access via an Evotrust iD are charged differently. In 2020, Evotrust was chosen by 52 municipalities (20% of all municipalities in Bulgaria) for their e-government-services.[2] The Evrotrust-integration into the portal of these municipalities allows citizens and enterprises to use e-gov-services of any of these municipalities, identifying themselves remotely with Evrotrust and signing documents with a qualified electronic signature (QES). The Evrotrust e-signature has the same legal value as the paper signature. Evrotrust uses advanced "3D machine-learning technology for automated face recognition and ID document processing" (see above). The app can be downloaded from Google Play or the Apple App Store. The app became somewhat popular in Bulgaria for applying for Corona state aids, but there are no numbers concerning the use of Evotrust e-signatures in Bulgaria available.

- Despite a big project to introduce a national digital eID which started in 2016, in 2023 there is no government-issues central eID available in Bulgaria yet. The award of the technical infrastructure was held up in a long legal dispute by the losing bidder until the year 2022. In the meantime, the introduction of a passport-based eID was attempted but failed due to administrative hurdles, and several attempts to combine the two approaches have failed.[3] In April 2023 the Bulgarian Interior Ministry announced that will issue new passports with integrated chips starting at the end of 2023. It was said that the assignment of a mobile application for electronic identification, which facilitates the use of electronic administrative services by the public, is an important aspect of this project. The contract was won in the public tender by a German consortium.[4] In general, political instability is hampering the introduction of a eID system in Bulgaria. Between 2021 and 2023 Bulgaria has seen five elections (April 2021, July 2021, November 2021, October 2022 and April 2023).

- Concerning e-gov services it seems that in Bulgaria many services are already being offered online but that they are hardly used by citizens because of the problems with secure digital identification. Usually, the infrastructure for electronic services (eID/ digital signatures) has to be available before e-services (e-government or e-commerce) can be used. In Bulgaria, it seems the other way round: Many e-government services already exist, but they are currently not widely used by citizens because there is not an easy-to-use eID/e-signature-system in place.

The reason why many e-government services are available in Bulgaria is that „the indicators are how many systems we have introduced, how much money we have spent, how many services we have. But nobody cares how much they are used, by how many people, how much time they have saved. This way of thinking has brought us to the point where we offer services, but they are not being used," said the former minister of e-government Bozhanov in an interview (Zapryanov 2022).

The assessment that Bulgaria already has a number of e-government services online is confirmed by the European Digital Economy and Society Index (DESI): According to the 2022 edition of the DESI report, Bulgaria has more than 852 electronic administrative services available online. Also, DESI states that in Bulgaria, the national public administration registries can exchange information electronically (DESI 2022, p. 17).

- Bulgarians seem to be reluctant to use e-government services due to data leaks in the past: There have been leakages of personal data by a large public administration in Bulgaria. As a consequence, citizens seem to be afraid of leakages of personal data and are afraid to use digital services, and especially public services (Simeonov 2022). In addition to the notorious data leak from the National Revenue Agency in 2019, in the last two years the country has been subject to numerous distributed denial of service (DDoS) attacks. In the DDoS-attacks, no data was leaked, but concerns in Bulgaria arose about the safety of the system as such (Zapryanov 2022).

- The is no information available about eIDs to be used in the health system in Bulgaria.

[2] https://evrotrust.com/blog/e-services-in-nearly-20-of-the-municipalities-in-bulgaria-are-already-available-through-smartphones
[3] https://blog.bozho.net/blog/4004
[4] https://sofiaglobe.com/2023/04/05/interior-ministry-bulgaria-to-issue-id-residence-cards-with-chips-by-end-of-2023/

Literature

- DESI (2022): Digital Economy and Society Index (DESI) 2022, Bulgaria, www.mtc.government.bg/sites/ default/files/desi2022bulgariaengagsggapyfhc84q8w4vxe2v11lq88692.pdf
- Simeonov, Georgi (2022): Peshtera – the Bulgarian pioneer administration to test new innovative methods for e-Identification of its citizens, 3 January 2022, www.impulse-h2020.eu/2022/01/03/ peshtera/
- Zapryanov, Yoan (2022): E-government: Time for an update. The new government plans radical digitaliza-tion of Bulgarian bureaucracy in its first year. In: KInsights, 21 February 2022, https://kinsights.capital.bg/politics_and_society/2022/02/21/4314535_e-government_time _for_an_update/

List of participants

The following people participated in the Bulgarian workshop:

Participant No.	Organisation	Session
1	RK D'ART EOOD	Use cases
2	MOP	Use cases
3	BORICA AD	Use cases
4	Municipality of Bratsigovo	Use cases
5	Infonotary PLC	Technology
6	Postbank	Law&Regulation
7	Sofia University	Law&Regulation
8	CCB	Law&Regulation
9	FIZ Karlsruhe	Law&Regulation

Table 9 Participants of the Bulgarian workshop

External experts participating: 9, from the IMPULSE project: 19, no break-out sessions

A.2 Documentation of the Spanish workshop on January 26, 2023

Title of the workshop:

Soluciones de Identidad digital en servicios públicos y privados mediante el uso de registros distribuidos e IA. IMPULSE descripción, casos de uso, requerimientos.

Who was in the workshop?

Hosts of the Spanish workshop were the coordinators of the IMPULSE project Jaime Loureiro Acuna and Xavier Martínez from Gradiant as well as representatives from the other Spanish partners Alice Biometrics, Tree Technology, and the pilot owner Ertzaintza from the Basque Government. Also, two experts from our Italian partner Cyberethicslab (Luca Mattei and Tetiana Vasylieva) were present to answer questions concerning regulation and standards.

The language of the workshop was Spanish, except for the break-out session on regulation and standards which was moderated by Luca Mattei and where participants were asked to switch to English.

The workshop was held online on January 26, 2023 from 10 to 11 o´clock. 20 external experts participated in the workshop.

Agenda of the workshop

The 1h-online workshop had the following agenda:

- Overview of the IMPULSE solution, including pilots (10 min)
- Technical aspects and questions (10 min)
- Three break-out sessions (technology, use cases, regulation and standards, 40 min)
- A wrap-up session at the end of the workshop (10 min)

The slides used for the presentation can be found in the annex.

Documentation of the break-out sessions

Use cases, user requirements and methods

Participant 1 exemplifies how this type of technology is used in the Autonomous Community of Catalunya. Through a service similar to Cl@ve called idcat mobile (used in the general state administration), it consists of a user with a one-time password that is sent to the cell phone and is registered by video identification. It is successfully accepted. Qualified digital certificates are also accepted and they are exploring other digital identity models based on blockchain and other technologies. As for video identification, it follows the associated order the electronic signature let that applies in the state that regulates how to make video identification to issue digital certificates. It can be done through an operator by videoconference or through an algorithm that detects the DNI and validates it against the National Police. Subsequently it is also validated by an operator a posteriori to issue the certificate. It takes approximately 5-10 minutes to register when the flow is normal.

Q: How is the validation process by an official at IMPULSE?

A: Validation by the officer is performed in the registration process. When a user is registered, a process of video identification and documentary validation of the ID is carried out using artificial intelligence algorithms. If both processes are successful, an officer must manually validate the process and the information to issue the ID card. In addition, this verifiable credential is stamped with QSeal.

Technology aspects

The IMULSE consortium explains the different modules that make up the IMPULSE solution.

Participant 4 asks about the role blockchain plays in this type of solutions. And what does this solution technically add compared to other technical tools.

A: A distributed service provides greater transparency than fully centralized systems in some functions, which would be more difficult to do otherwise. Such as, who are the trusted emitters or which are the certifying organizations, what can they be trusted emitters for, the reliability of the solution, it does not give access of private data to the emitter. It also gives autonomy to the user in the public service landscape. In addition, distributed registries make it possible to make the verification of credentials independent of their issuance. That is, an entity can verify the credential presented by a user in the DLT without the need to consult the emitting entity. In this way, the issuing entity does not know the services to which the user is connected. Carlos comments that DLT technology is not strictly necessary for the implementation of an identity model, but it does provide greater transparency and control to the citizen than fully centralized systems.

Comment by participant 5: Potentially, the issuer has no control over how, by whom or when this information is consulted, but it seems a chimera to think that users and citizens are really autonomous in the consultation of this information, because no citizen, no normal person is able to consult any information in a blockchain if it is not through a system that is provided by someone on a phone, such as an application, a cell phone, a platform of a provider, a private company or the public administration itself. In short, the problem is not in the form in which it is stored, the problem is in the means that you have to consult this information.

Comment by participant 7: There is no strict consensus with blockchain, since only the issuer can modify what has been issued but not the end user, who can only revoke. There are status changes in which there is an agreement between the participants that are correct, but it must be understood that there is no consensus. This participant does not see a strict need to use blockchain.

Impacts, regulation, standards and politics

Question from IMPULSE members: How do the participants see the regulatory horizon for enabling and allowing new electronic identification models based on more disruptive technologies such as those used in IMPULSE?

A: Participant 16 is a member of ETC ESIF Standardization Technical Committees related to trusted services and media and director and coordinator of the standardization project to create a European technical specification for decentralized digital identity based on DLT in CEN CEL JTC 19 WG1:

- The most optimistic regulatory horizon would lead us to the approval of eIDASv2 in 2023. This estimate is very optimistic, and we will be able to assess it better when the European Parliament has approved its negotiating position. In the current state we have the proposal presented in June 2021 and the recent approval of the general orientation of the Council of the European Union which is the mandate for the trialogues. If the Parliament adopts a position relatively close to that of the Council, possibly, the trialogues will be agile and will be approved quickly. However, assuming that it is finally approved by the end of 2023, the availability of the digital identity portfolio by governments would take us to 2027 because of the time involved in the RF implementation acts and procedures.

- However, he does not consider the real bottleneck to be there. In his opinion, the bottleneck is that there is no certification scheme for remote biometric enrolment. He is aware that TC224 has sent a DGCONNECT letter stating the need to evaluate work in this direction. This causes a major policy discussion on the wallet because it is a high-level electronic identification medium. The big problem lies in the fact that there is no established procedure for remote biometric enrolment, and there is no technological certification scheme to help this type of solution. Therefore, two proposals arise from this for the board going forward:
    1. Determined by national regulations on electronic identification means, where the focus is possibly more on the face-to-face environment. In many of these mechanisms they have to obtain reliable biometric information.
    2. Substantial (not high) level identification mechanism where solutions such as IMPULSE together with additional complementary measures, i.e. compensatory controls that will have to be decided, would be more appropriate in his opinion. The time to consider this type of tests and technical controls is now. He suggests that IMPULSE should have strong interaction with TC 224.

- On the issue of using electronic ledgers as the underlying technology for digital wallet implementation, such as EBSI, a proposal has been developed and negotiated with the Council. Ignacio is very pleased that it has survived, and it seems in his personal opinion that there will be a regulatory framework for trusted blockchain. In his opinion this enables the possibility of being able to qualify EBSI to be eligible to support the trust translation elements of the system to be able to aspire to have decentralized registries of issuers as an alternative to trusted lists, which will take quite a lot of discussion in the standardization committees. Ignacio Alamillo clarifies that in his opinion this is the will of the technical committees, but it will have to be formalized by the relevant institutions. On the issue of using electronic ledgers as the underlying technology for digital wallet implementation, such as EBSI, a proposal has been developed and negotiated with the Council.

Spain: Background report

In Spain, there are two eID systems that can be used nationally for e-government services: the electronic passport (DNIe) and the Cl@ve-system (Clave is the Spanish word for „key“).

- An electronic ID card with an integrated chip was introduced in Spain back in 2006. Since then, there have been several revisions of the technology. In 2021, version 4.0 of the DNIe (Documento Nacional de Identidad electrónico) was introduced. In 2023 citizens still need a smart card reader and a PC to use the DNIe as a means to identify at e-Government platforms. However, the new DNIe also includes NFC technology which enables it to be used as a mobile means of identification. As part of the Spanish government's España Digital 2026 programme, the use of mobile identification via smartphone is planned in the near future. The "DNIe en el móvil" (DNIe on the mobile) project continues to be under development in mid-2023[5]; a launch date has not yet been specified.

- In Spain, although there is no central e-government platform, there is a central service for authenticating citizens to the various e-government websites. This authentication system is called Cl@ve. The Cl@ve system is designed to consolidate and simplify electronic access of citizens to public services, allowing them to identify themselves through concerted keys (user and password). The system is offered in two variants: For sporadic users („Cl@ve ocasional“, using a one-time-PIN) or for regular users („Cl@ve permanente“ with a permanent password).

To register to the Cl@ve-system, users have different possibilities: They can visit their local administration in person and apply for a Cl@ve ID via paper documents or they can do it online using their tax certificate or the DNIe with a card reader on a PC, or they can apply for it using a videointent procedure. Once registered, Cl@ve users receive a PIN on their mobile phone via the Cl@ve-PIN-App each time they log in to a Cl@ve certified service. Public administrations in Spain have committed themselves to gradually open their services to the Cl@ve system. In 2021 more than 7,600 e-government services had already integrated the Cl@ve as a means of authentication (eID Strategies 4 2021, p. 83).

[5] https://espanadigital.gob.es/en/lines-action/new-digital-identity-model

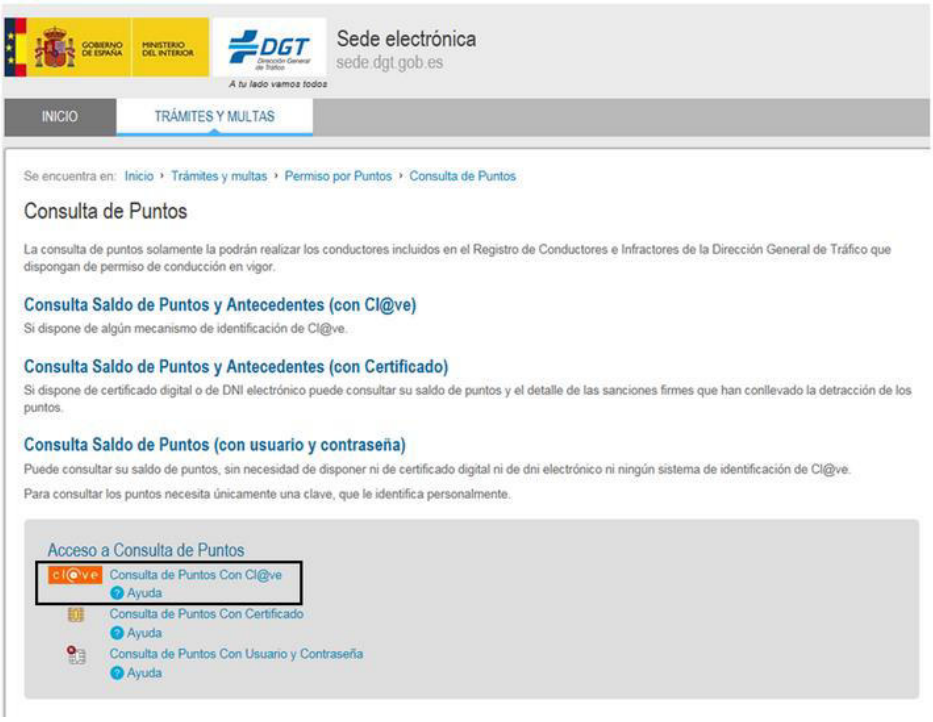


Figure 4 Cl@ve icon integrated in an e-gov Website

Source: https://clave.gob.es/clave_Home/en/clave/funcionalidad.html

Figure 5 Identification options of the Cl@ve system

Source: https://clave.gob.es/clave_Home/en/clave/funcionalidad.html

Public administration services requiring identification have integrated the Cl@ve icon (see figure 1 above). After clicking on the Cl@ve icon, users will be redirected to the (see figure 2).

A Cl@ve ID IDs can be used for a variety of e-government services, such as changing addresses, viewing traffic tickets and penalty scores at the Spanish traffic authority, processing tax returns, applying for the extension of unemployment benefits or using the social security online platform Import@ss. At the end of 2020, almost 11.5 million citizens had a Cl@ve ID according to the Spanish Digital Public Administration factsheet of 2021 (European Commission 2021a, p. 10). Nevertheless, in the Wyman-Report of 2021, the adoption of eIDs in Spain is estimated to be below 5% of the population.

In addition to the two national eID systems, there are several regional and even municipal eIDs available in Spain. Most of them are Citizen Cards („Tarjeta Ciudadana“) issued by the local administrations for example in Gijon, Palma, Zaragoza or Alicante. The Citizen Cards can not only be used for e-government services but also for public transportation and when using public facilities such as swimming pools or libraries as they have an integrated payment function.

In the Catalunya region, the Meva Salut App allows health services to be accessed online (diagnostics, medication plan, making appointments with Primary Care Centres, communicate with healthcare professionals and ask questions about health issues that do not require in-person or urgent care).

In general, in Spain there are many regional and municipal initiatives for bringing services online and for providing secure identification with specific eIDs. An integration into a central standardized system does not seem to be planned at the moment.

Sources

- European Commission; Deloitte (2021): Overview of Member States' eID strategies. CEF eID SMO Version 3.0, January 2021. Authors: Massimo Pedroli, George O'Neill, Arianna Fravolini et al.
- European Commission (2021a): Digital Public Administration Factsheets – Spain. Brussels, DG DIGIT and DG CONNECT, Prepared by Wavestone, https://administracionelectronica.gob.es/pae_Home/dam/jcr:6eeb139e-76b0-4d18-8a27-46e23c87fbe6/DPA_Factsheets_2021_Spain_vFINAL_0.pdf

List of participants

The following external experts participated in the Spanish workshop:

Participant No.	Organisation
1	Project Manager at Consorci Administració Oberta de Catalunya
2	Veridas
3	Veridas
4	Cluster TIC de Asturias
5	Alastria
6	Alastria
7	Logalty
8	Head of Blockchain Strategy, Inetum - Digital Identity Leader, Alastria - Identity Expert at ESSIF-EBSI, European Blockchain Partnership
9	INETUM
10	FADE
11	UnicajaBanco
12	Responsable de innovación en Seguridad del BBVA
13	AYUNTAMIENTO DE GIJON - PROMOCIÓN EMPRESARIAL Y TURÍSTICA DE GIJÓN S.A.
14	CTIC Technology Centre
15	DPO & IT LAW
16	Member of ETC ESIF Standardization Technical Committees related to trusted services and media and director and coordinator of the standardization project to create a European technical specification for decentralized digital identity based on DLT in CEN CEL JTC 19 WG1.
17	Software Specialist
18	Head of Safety at Euskotrenbideak-Ferrocarriles
19	Director of Technological Development
20	no affiliation given

Table 10 Participants of the Spanish workshop

A.3 Documentation of the French workshop on February 23, 2023

Title of the workshop:

Identity Management in PUblic SErvices. Identité numérique et services publics. Quels technologies, moyens, impacts et future exploitation ?

Who was in the workshop?

Host of the French workshop was Bertille Auvray from Pôle TES. She and her colleagues Marie Pereda and Benjamin Cheret had invited a group of French experts for eIDs and related topics. The language of the workshop was French, whereas experts from the IMPULSE project were also present to answer technical or regulative questions in English by request.

The workshop was held online on February 23, 2023 from 10 to 12 o´clock.

14 external experts participated in the workshop.

Agenda of the workshop

The 2h-online workshop had the following agenda:

- Short presentation of the IMPULSE project (15 min)
- Questions and answers concerning IMPULSE (5 min)
- Three break-out sessions (technology, use cases, regulation and standards) in two rounds (session 1 from 10:30 to 11:00 and session 2 from 11:00 to 11:30 hrs). The break-out sessions were introduced with a presentation of the IMPULSE identification process and the IMPULSER pilots. Participants introduced themselves to the group. After session 1, participants changed their group so that different aspects could be discussed in small groups (30 min for each of the two sessions).
- A wrap-up session at the end of the workshop (11:30 to 12:00 hrs) was foreseen to summarize the results and to present further steps (30 min).
- Summary and next steps (5 min).

The slides used for the presentation can be found in Annex B.

Documentation of the break-out sessions

Room 1: Technology aspects (sessions 1 and 2)

P(articipant) 1: Facial recognition at the time of use of the service, will there be a need to connect to a server to make the comparison (between recorded and live image). This is an important point to mention about how the data is collected + stored (transparency).

P2: He noted the importance of the notion of transparency for the user (in response to P1). He then presented 3 points:

- User experience: will the tool offered to citizens be as effective as a dating app, for example, which allows a very fast connection. There is the question of fluidity.
- Ideological issue: creating adhesion both through the experience of the tools and platforms and the interest that it can have (which is what the big brands know how to do, for example). How can the public administration manage this without going into the "flashy" as the brands can do. Ex. France Connect, very little support.
- Transnational mobility: How can a tool like this be developed to be used taking into account the mobility of the citizen at European level. Do not limit yourself to the services of your territory. How can we imagine approaches in other European countries?

Question about the ubiquity of the IMPULSE application.

P1: For the European aspect, it will necessarily be necessary to take into account the aspect of data interoperability and it will necessarily be necessary for Europe to give an impetus with an agreement of all the European countries with a common method of transfer and recognition of security and data certification.

P4: Question about the governance model by going through EBSI, is it really decentralised? By using a private blockchain, we lose the decentralised aspect and it is no longer really in the hands of the citizens.

See what Vitalik Buterin (Russian-Canadian computer scientist) has done about the new tokens he has made that are used for a unique identity to each individual (like NFT that cannot be transferred) to prove his identity. Also look at Web of Trust (connect with people who validate identity without having to go through institutions. Linking with people close to us and by looking at the network we can find out who has impersonated us because their network is closed to the outside world. For example, the links with Facebook, we can find this pattern of relationship with others, which we do not find in someone who has impersonated an identity. The social aspect is also favoured because we go through human links and this can also help to recover a lost identity (other than the use of facial recognition with AI, which can potentially be falsified with digital advances). We still have the notion of a password, but if it is lost we can ask several people to confirm the profile (linked people), which will generate a new password. = distributed identity + security thanks to links between humans, we digitalise but maintain social links.

P1: Major security issues, because for example on the sites of a bank we are still going to propose anti-robot tests with images when it has already become obsolete and it is not certain that the institutions are aware of this.

P5: What about the administrative slowness (at national and European level) for the implementation of interoperable systems?

P4: The question of interoperability is a major issue. According to him, we should not underestimate the potential of AI to allow interoperability between systems. Now what we do with AI is to convert data to another type of live data (e.g. post on LinkedIn, and the AI reduces it directly for Twitter). We don't necessarily need one format for all, but why not rely on AI to convert between different systems in real time. The possibility of proposing IMPULSE in Europe is to say "even if there is no interoperability, the AIs will be able to do it live, and therefore no longer have the "winner takes all" situation with a monopoly that takes everything". This could avoid the bottleneck that we have had with, for example, VHS and BetaMax, DVD and Blu-ray, etc. and the quest for a monopoly.

P3: Social score: a key subject which is also linked to interoperability, is that of social score. Today there is a democratisation of the concept of social score which goes into all interoperable systems because by giving power to external parties we can give them the capacity to denounce / isolate / segregate. E.g.: use of a public transport ticketing service and forgetting to punch in. Incident recorded in the database. How to take into account that this will not affect other services offered?

P8: The first point is to be careful with the principle of societal inclusiveness, it has to work with all people. How is the robustness evaluated for people with skin problems, a damaged eye, etc. but also simply on the skin colour of the people.

Will it give the same result with the AI, bias if it has been trained with a certain type of person. It is important to check this for the societal aspect. The other point is on the security aspect, each state has its own group that will give labels guaranteeing the respect of security. Does IMPULSE plan to go through an evaluation to obtain a European label? This would give confidence in the solution because it would have been validated.

E.g., ETSI TS 119 461 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf

FIM Research Unit: proposing research papers on bias, assessing the impact of bias and working on the design of a common label to ensure robustness against societal bias.

P7: What type of blockchain is ultimately targeted, what will be its role and what elements will eventually be stored? When we talk about interoperability, we are also talking about trust in the data and that not all stakeholders necessarily want to distribute their data to the entire ecosystem.

P5: What about the system during the lifetime of a person? Faces obviously change and we are talking about facial recognition. But also the question of after death. Will the relatives have to do something (reference Web of Trust).

P6: For example, to ensure security at the nuclear power plant (private domain case), the biometric data is stored for only 3 months. This period slips with each use, but without use for 3 months after the last use, the data is permanently deleted and the registration process will have to be repeated.

Room 2: Use cases, user requirements and methods (sessions 1 and 2)

Q: Which of the presented pilots or use cases are you most interested in?

P12: Interest in the Icelandic case, especially on the issue of access for citizens in fragile situations, for the Red Cross.

P9: Interest in the case of Bulgaria, to see how we accompany citizens, how we can help them to get involved in this, the questions of confidence in services, but also accessibility (e.g., recent study showing 17% of e-illiteracy) so how can we accompany the remote public?

P10: Similarly on the subject of e-illiteracy. But also the question of voting, at the level of local authorities because it is a very important subject (case of Gijón). We can see a real resurgence in the willingness of local authorities to commit to the issue of citizen participation, participatory democracy, etc. So how can we go about this? So how can we go as far as voting, because today we are more on the question of consultation.

P11: As a citizen and not a member of the administration, I am interested in electronic voting and filing complaints online.

Q: What are the main use cases for digital identity solutions in France?

P9: For the moment, what we can indicate is identification via the email address and password to access a service to go to a library account. And on the authentication part, this requires being able to scan an identity paper or facial recognition, there had been projects at government level which did not succeed because this posed the problem of biometric identification, particularly at the level of the CNIL.

So it is not currently used in public services, or only on an experimental basis. For example, in a high school in Marseille, where a facial recognition system had been set up at the entrance to the school. But there was a lot of controversy and it had to be withdrawn. In the example of the Rouen metropolitan area, it is more a question of identification, with the water portal for paying your water bill with a login and password.

P12: Currently, the French postal service (La Poste) offers this principle of online digital identity, with double authentication (or even triple authentication), as with banks. But we can quote Elon Musk, who said that text messaging is not the most secure way to verify identity. Within the Red Cross, we are encouraged to support users in using the authentication principle. Even if we are not encouraged to use it, if we refuse the principle of double or triple authentication, we will have to go.

Q: So what La Poste is offering is different from France Connect? Is it even more secure?

P12: Yes, it's different, it's a digital identity here. But it's quite recent and we're hearing more and more about it. The difference with France Connect is that there is no secret code directly attached to this service.

P9: It is a federation of identities, not requiring us to have a multitude of identifiers but to use the identifiers of the Tax Office to use another service. But there is no code to make it even more secure.

P12: Online live test of La Poste's digital identity - seems to be an equivalent of IMPULSE in terms of an add-on to the public service site, but still requires a password sent by text message, then you have to validate access with the code you receive or by fingerprint.

Q: What are the main requirements that digital identity solutions like IMPULSE must satisfy to be widely adopted?

P12: Mandatory RGPD. And obligation to generate trust. For example, China has implemented this principle of facial recognition in the street. For the time being, there is no real question of this in France (note Bertille: it happens in certain private places), but if we change the person in power, could it become a reality? The question remains that of controlling the population. So there should be a RGPD (or equivalent) which would indicate that any power could take control of these tools, held by the public administration.

P9: The RGPD is supposed to provide a framework for this principle.

P12: In the context of the development of such a solution as IMPULSE (or others), this would necessarily have to be included in the RGPD or another text.

P2: Interest in the case of ARH. We can also make the link with people who are not necessarily homeless but who may be concerned by nomadic life (example of the participant living in a camper van for 3 years by choice). Important domiciliation issues. The notion of a safe is therefore very important to consider.

Q: What are the main requirements that digital identity solutions like IMPULSE must satisfy to be widely adopted?

P1: We should not underestimate the user requirements, because this is something that is often done (e.g. France Connect, which is not complete). This is done in a multigenerational way. For young people, it has to be fast, efficient and secure (the habit of a very well thought-out application, with immediate information on connection to the service), and for older people (to get round their reticence and catch them in the digital wave).

P14: I completely agree. In the profession of notary, in a very rural commune, we regularly come across elderly, vulnerable (or even very vulnerable) people who are completely side-lined just by the notion of the Internet and digital technology. There is a real problem in rural areas, there is a total absence of public services. Perhaps in the long term, we could use notary offices to play the role of accompanier, in rural areas, for people outside the digital loop. With perhaps a computer at their disposal, the notary's ability to certify a person's identity (and therefore why not to certify it online for procedures). This could also make it possible to have a friendly reception area for older people and therefore to maintain social links, to keep a person present in person, while using digital solutions.

P14: On the question of the digital divide, we find this point of rurality with this digital desert and digital support. There is also the issue of taking into account citizens who are visually impaired or very disabled. They may be the forgotten ones in these digital solutions because they are deprived of certain means. In the dematerialisation and digital access processes, almost everything depends on the user himself and there is little support. We can therefore envisage a centralisation of services.

Question on filing a complaint: does the justice system follow suit? In the justice system, there are real questions about the digital tools of the justice system, particularly with the forthcoming publication of the plan for the transformation of the justice system, which should be published soon.

Also, the important point to remember is confidence in digital identity systems, which explains a lot of reticence. Particularly with regard to France Connect, the users have a rather good vision, but on the other hand, for private procedures (of a company), the company managers do not really want to use their own name when it is in the name of the company that the procedures are carried out.

For example, for architects' studies. Often the architect gives the information to someone in the firm who has to transcribe the information. However, the employee must use the architect's personal information. This raises concerns about security, trust and responsibility.

P2: Supporting P13's speech, in relation to the level of negligence of the human. We have AI arriving on the French market (e.g. ChatGPT), which has the potential today to help users, particularly the visually impaired, and will make tools less expensive (by disrupting the market). And this AI could potentially also compensate for the absence of human support, as one can imagine 100% efficient virtual assistants. However, the possible pitfall is to continue to neglect the human. AI can help to compensate for certain deserts, but we can also take advantage of putting humans back where they are really needed and therefore use AI for tasks that can be outsourced.

P13: We can also think of the problem of deep-fake and voice-fake. The newspaper Le Monde published an edition of General de Gaulle's speech of 18 June 1940 and it showed that they had managed to remake his voice. If tomorrow we ask someone to put himself on video and to take an image and voice of someone else. Can we think about having a barrier to avoid this and still guarantee security?

P2: On the bank's sites, we have the principle of anti-robot security (recognising a traffic light, a bicycle, etc.) which has become totally obsolete. Having worked, before becoming an entrepreneur, in the air force and space, in a secret defence division, on electronic warfare and computer hacking. It always comes down to the same thing, the more viruses we have, the more anti-viruses we have, the more viruses we have, etc. and it's endless. To counter this, we have, for example, the recognition of the social fabric (family, friends, etc.). It is almost always possible to falsify a fingerprint, a voice or a face.

Q: What are the main challenges to the adoption of new digital identity solutions like IMPULSE?

P13: Within public services there is a real need for training and acculturation, because agents are not familiar with these new technologies. We're talking about territorial agents here, these technologies are not in their core business.

Room 3: Impacts, regulation, standards and politics (sessions 1 and 2)

P8: In relation to the RGPD. Who has access to the data at the time of the face + ID photo? How long are they stored on the server? How are they secured?

P14: In the context of the notary's profession, there is necessarily confidentiality of information, however, beyond the use, there is no technical knowledge behind it. This technical part is done between the organisation that manages the delivery of the service and the IT service providers.

What is important to note is obviously the question of data security, whether it is national (within countries), but also at European level and in some cases even international, which will then come under private international law.

We also need to find the most sophisticated solution possible, because we are seeing an upsurge in cyber-attacks on dematerialised exchanges in the industry, but also elsewhere, which inevitably leads to the implementation of an increasingly high level of security.

P7: It also depends on what you want to protect against, there is a difference if you stay on the digital identity or if you talk about the attack on a computer system. In relation to identity, there are things that exist today

that allow a natural person to be able to prove that he is the author of a document and guarantee this to the recipient, thanks to cryptography (cryptographic key system), blockchain being one of them.

P14: On the aspect of verification of identity, it is true that the possibilities are there and that we are less backward than on certain other aspects. In the notarial field, a means of making remote notarial powers of attorney by videoconference has been set up for the creation of authentic notarial deeds (to be distinguished from a "simple" signature). This assumes that the identity of the person is verified beforehand.

There are two possible ways of doing this: either the notary has met the person within the last 10 years, in which case he or she can legally initiate a procedure to verify the person's identity at the beginning of the videoconference (by sending and signing a document digitally live), and then the document can be signed online; or if it is more than 10 years old, an external agent (DocuSign) can be used to verify the identity, in which case the notary can initiate a procedure to verify the person's identity. It is generally noted that the dialogue with the client is rather complex and not very fluid between the client - the external agent - the notary. This identity verification phase is rather confusing, which does not really encourage the notary to use it.

The idea for this part would therefore be not to use an external agent but to pass directly between the client and the notary. Either via a solution like IMPULSE, or with a solution that can be used directly between the client and the notary. It would therefore be interesting to be able to provide the notary's world with a reinforced solution and not to leave it to a third-party certifier who brings nothing to the file.

P7: It must be taken into account that these people are qualified to do this work. However, it would obviously be possible to set up a system whereby the notary has his own Qualified Web Authentication Certificate (QWAC).

P13: Having a solution such as IMPULSE (or other) would be a step forward in the notary's world in terms of both security and fluidity of exchanges. This would save time and would also allow even greater control of the files.

P8: The question is also, in these cases, who is responsible in case of fraud? Is it currently the third party who does the verification (and who says he confirms the identity of the person) who is responsible? And if it is the notary, would the notary be responsible for the fraud?

P14: For the time being, it's a joint and several liability (liability *in solidum*), so the liability would be on the third party but all the people involved in the case would be impacted. From the moment there is a prejudice, a court will condemn all the agents jointly. This does not necessarily suit notaries, since their liability is engaged by a third party and it would be preferable to recover the burden of identification in order to engage only their own liability.

P8: New question on national recognition, for official documents it must be recognised by sworn agents (currently the ANSSI - Agence nationale de la sécurité des systèmes d'information (i.e., National Agency for the Security of Information Systems) which does this). Could IMPULSE serve as a certifier?

P13: This issue is beyond his remit, however, mention was made of the agreement between the notary's office, the French government and DocuSign, for the agreement on the process. Secondly, on the recognition of the final document, as it is a notarised deed (the highest level of recognition), it is already recognised at national level.

P8: Exactly, hence the need to guarantee the identity of people at a distance.

P14: Indeed, if there is identity theft, this can significantly weaken the relationship (to be put in the context of the AP and the user as well, where the weakening/loss of trust in the service would be very detrimental to the latter).

It is necessary to ensure that the system, from the outset, is not flawed. For example, there is growing fraud in the sending of bank details (RIB in French) on the Internet. If there is to be an exchange, it must be done by hand with a counter-signature.

P7: Bank statements should be certified by the companies, or at least made verifiable so that a notary could be able to check them.

P14: Currently using RIB verification platforms, which seem to work for companies. But in the case of the notary, the clients are very often ordinary people who are not necessarily able to have their document certified. Sometimes even sending over the internet is complicated, so using a platform would make it even more difficult to send and obtain documents. We are still left with the method of hand to hand collection (i.e. physical movement) and therefore the opposite of a fluid solution, as proposed by IMPULSE, and we remain with a basic solution.

P7: Finally, to sum up, we can see that the problem is the trust we place in the data we receive. We could then have this principle that it is not the individual himself who certifies but the banks who take charge of setting up the certification of the RIBs they issue. It is the general ecosystem that must take on the digital culture and therefore not put the whole digital chain in the hands of one person. This would also allow the use of digital solutions even in complex ecosystems.

P14: It's true that we're currently in an intermediate phase, which can be dangerous because we're not at the end of the process and so there are more or less significant flaws.

The recommendations we have at the moment are that if we receive a bank identity statement, we still have to phone the client to be sure of the references of the RIB to check the information on it.

P7: On the question of trust in the eID as a signature (QSeal), it can almost be said that a paper signature has less value than a cryptographic signature. Before being a printed paper, it is a digital document. So this digital signature can suffice and certify the document just as much. On the question of qualifying the eID based on biometric recognition as an electronic signature, we still have to discuss this, but the cryptographic signature has a strong value.

P8: There is an upsurge in the use of these digital options. We see this with the digital wallet. However, once again, it is important to emphasise the security of this, the protection against types of attack, etc. In particular with biometrics and facial recognition, there is morphing. How can we evaluate the false rejection or false acceptance rates? How are they checked? Also, the question of the demographic aspect, how will it work with different types of citizens (skin colour, etc.). Again the question of trust in the system is important, especially if the eID based on biometric recognition becomes a qualified electronic signature.

P7: On the question of biometrics, it is difficult to say. But in any case, the cryptographic tools that are used today (pair of keys that allow a document to be signed) are robust. They have never, until now, been broken. So the question is, will quantum computing be able to overcome this robustness, in a few years perhaps, but for the time being what we can guarantee is that a signature that has been cryptographically signed cannot be corrupted as long as the person signing holds his secure key card and does not communicate it, in no way will a third party be able to falsify the signature.

Q: What are the main legal and regulatory requirements that a digital identity solution like IMPULSE must meet in France, including certifications?

P10: Given that it is a European solution, the first requirements to be met are necessarily European regulations, so necessarily the RGPD or EDAS. It is clear that if we have to have a European-level solution, it is the European regulation that must govern the solution.

P1: The acceptability part must also (and above all) be taken into account, because any product/solution can be made, if nobody wants to use it, it is useless. We can see that the French government has already made

many attempts that ended in failure, because they did not take into account the user himself. It is imperative that there be an ethic of use and secure data management with a fluidity of use so that people understand above all what the product is for.

In the context of another project, at national level, P1 had set up focus groups to find out who the participants would trust to manage their digital identity: telecom operators, banks, the State or local authorities. For telecom operators, they were rather afraid of commercial exploitation, for the bank it was anyway the use of the individual's identity as issued by the bank, for the State the fear came rather from the fact that it could become "big brother", and therefore the trust, unanimously, went rather to the local authorities because it represents the place of life, proximity, trust in elected representatives and the administration. It is essential to take this into account (the proximity aspect) when deploying something. On the other hand, the regulations must come from the State or the EU. And it is imperative to put in place a very important security system, because it would be very serious to steal all the community's eIDs.

P10: So there is both a technical and a human challenge when you want to implement a solution like IMPULSE.

Question for P11: In the banking sector, you are used to using electronic safes and eID. How is this use perceived by customers?

P11: We found that customers were not very inclined to use the electronic safe, and there was a fear of piracy and misuse of the data, despite the fact that it was clearly stated that the information was not stored with one's own identifier (traceability). Similarly, this low usage was also probably due to the fact that bank advisors do not necessarily trust this service. It was therefore difficult to "sell" this service without 100% adherence.

P1: It is true that this low use can be explained by fear, and this fear can be explained by the fact that there are few or no use cases on which to base an example. We can also see that technology is evolving very quickly, but on the other hand customs and habits are evolving slowly. There is still a tendency to use material things a lot (the classic paper and pencil duo). But we can also present the use of a simple cloud for example as a means of safeguarding against a fire (e.g. important paper documents).

Q: Can a biometrically-based digital identity like IMPULSE be used as a Qualified Electronic Signature?

P1: I think that the electronic signature is used more and more. As for biometric recognition, it is also used more and more. So why not combine the two? But it has to be used for several purposes and not just one. If there's only one, again, it wouldn't get off the ground, but with multiple uses, it's going to be easier to get into the habit. Until perhaps the day when there is a huge case of fraud, which can disrupt usage.

P10: To date, I don't know if people are aware that biometric recognition can be used as / or become an electronic signature. To be aware if it has the same value as a paper signature.

P1: For the time being, biometric recognition is primarily used for identification and not for signing. However, as soon as you really identify yourself, and you are sure that the person identifying himself is the right person, it could be considered as a signature, and therefore there would no longer be any need to add a new signature stage (the two would merge).

Comment moderator: If we compare the answers from this session with those from the previous session, we can see a difference because those from the previous session, in their job, were already aware of the shift in usage by users and that biometric recognition is therefore already recognised as a signature that cannot be corrupted.

P1: Perhaps we should also take into account the moment of signing, perhaps when people are going to sign, as they have already had to use biometric recognition to authenticate themselves, so why not use it to sign as well.

P10: It may also be a question of acculturation.

P1: That's why it's important to do an acculturation by level according to the people. But it's not easy to talk about security and trust like that without getting into the complexities. And we also see that unfortunately some people do what they shouldn't do because they are not aware of the scope of the actions. E.g. "it doesn't matter, I have nothing to hide", whereas all data can be exploited. We can also mention the use of facial recognition cameras for security. But safeguards are needed to prevent this from becoming constant surveillance. The same goes for applications that use this method to identify themselves and access the service, so that it does not become a form of surveillance.

P10: It is clear that this must be taken into account, especially at the level of the State. At the level of local authorities, there are currently many initiatives by administrations (inter'connectés or FNCCR - Fédération nationale des collectivités concédantes et régies, i.e., National Federation of Local Authorities) that train elected representatives on these digital issues. This may also explain why people have more confidence in local authorities. There is a difference between the more national and the more local elected representatives, who are acculturated to both local needs and digital issues and therefore to the reality on the ground.

Q: In your opinion, in the private sector, who should play the role of intermediary to acculturate companies? Is it the technology providers, or is it cluters like TES?

P1, P10, P11 agree: A bit of everyone, each playing a part in the chain.

Q: What can the European Commission do to support the diffusion of digital identity solutions?

P1: At the level of the French State, it is managed by the Ministry of the Interior, which does not necessarily have the same objective as the others. Their objective is security, surveillance, very regal actions. In this framework, identity is treated as a tool (e.g. identity card). It is a rather centralised vision that does not necessarily put itself in the place of the people and therefore the solutions put in place do not work.

P10: As an individual, what could make me use such a solution is the confidence in it, the certainty that there will be no subsequent slippage with the use of the data and the use without the individual's knowledge and no longer having control. For example, that my data does not end up in a cloud outside the EU without my informed and explicit consent.

P1: When we developed our solution at Idhétic (i.e., his company), we started from the same principle as IMPULSE. We noticed that centralised solutions were being used, whereas it was important for the holder to remain in control of his data. In particular, we see examples, in the private sector, of companies that offer so-called identity systems, when in fact they are only identification systems (e.g. e-passwords) and which are centralised somewhere on a cloud that are regularly hacked. This is very serious because it makes it even easier to steal identities and to trick people. It is therefore important that the bearer remains in control of his or her data, with systems and techniques that allow data to be distributed when needed, but always with the control and consent of the person.

P11: Question on the existence of a solution in France (i.e., France Connect) and we can imagine that each country has its own solution. Is IMPULSE intended to replace all these solutions?

P1: It should be noted that France Connect is just a means of connecting and not an identity provider. Moreover, the use is quite complex, the ergonomics are heavy. And people find it hard to understand and may be afraid to connect via their tax password to another administration: where is the limit of information sharing?

P11: At the local authority level, we offer the France Connect service as part of a support package to carry out a series of procedures, which may be linked together. But here again, we provide support, people are not alone.

Background report: France

In 2023, French citizens can use more than 1400 public administrative services online through the „FranceConnect“ system. FranceConnect is a centralized access portal for public services. Users can identify themselves in different ways, for example by using their username and password that they use for the French tax website or by using their La Poste eID, issued by the national postal provider.

In 2021, the French government started to issue new ID cards for its citizens on which personal and biometric data is stored. The new ID card, called CNIe (Carte Nationale d´Identité électronique), is planned to be used as a means for identification at the FranceConnect portal. The system to log into FranceConnect using the new ID card is called SGIN (Digital Identity Guarantee Service or „Service de guarantie de l´identité numérique“) and works like the German system Ausweisapp 2 by holding the ID card on the backside of the smartphone where ID data is transmitted via NFC and used to identify the user and to unlock the services (Phillips 2022). The SGIN app, also called „France Identité“, is still in a test phase, a date for the official launch has not been provided (Elina S. 2023).

Figure 6 The portal of FranceConnect (screenshot from 2021).

Note: Portal does not yet show the possibility to sign in via “France Identité. Alicem was terminated in 2022.
Source: Gupta 2021.

A screenshot of the portal from 2023 shows that there are new possibilities for identification.

Figure 7 The portal of FranceConnect (screenshot from 2023)

Source: Bertille Auvray

The FranceConnect platform can also be used to connect to the Ameli health insurance account. „Ameli“ is the app of France´s national health insurance which allows its users to keep track of payments made to doctors or chemists, to update bank or postal details, to apply for complementary health insurances or to register the birth of a child. The Ameli portal itself can be accessed using the French Social security number. By using the

FranceConnect platform, users can access other websites as well, e.g. tax website (impot.gouv) using the same identifier plus password as used for the Ameli portal.

FranceConnect is aimed at simplifying the connection to many websites of official bodies and utility companies to carry out formalities. Thus, having an account at one of the main partner sites (La Poste, Ameli, tax office etc.) enables to users to access all the sites set up to use FranceConnect. As a security mechanism, the FranceConnect service consults the national statistics database RNIPP to check if the person's identity exists and he or she has not died.

According to the FranceConnect Website (https://franceconnect.gouv.fr/) there were 40 million users at the end of 2022 and about 1400 services available via the platform. The platform includes public websites of cities, departments and ministries. Services available include civil registry, retirement and pension, tax, health, justice etc. (see European Commission; Deloitte 2021).

In 2022 a more secure version of FranceConnect was introduced, called FranceConnect +. The enhanced version of the platform allows to use administrative services requiring a higher degree of security: banking services, electronic registered mailings or health services, like sharing medical records. FranceConnect + meets the requirements of the eIDAS regulation and allows substantial and high levels of approval. To use the high security requiring services via FranceConnect +, currently only the La Poste eID and in the future the new ID card app (SGIN) can be used. Other eID service providers may follow in the future (Balian 2021).

La Poste is the leading identity provider in France. To receive a Identité Numérique La Poste, an account has to opened which requires a French ID card or passport to be shown at a personal visit at one of La Posts offices. Once signed up, the person will be asked to enter his or her mobile number to receive a text message with a four-digit number which has to be typed into for verification. The La Poste eID works for e-gov, e-health, energy, vehicles, diploma, etc., it can be used in the same way as IMPULSE (see screenshots).

eID systems using facial recognition seem to have a difficult stand in France. In 2019, the French government was the first European country to introduce an eID system using automated facial recognition. The launch of the ALICEM-system ("Authentification en ligne certifiée sur mobile") was accompanied by massive criticism from data protectionists, IT security experts and civil rights activists. The ALICEM-system, which was developed by Thales´owned company Gemalto, used the information stored on the chip inside the old French passport which was to be scanned by the user with his or her mobile phone. The passport ID information was combined with a video selfie which the user needed to shoot in which he or she had to film himself or herself from different angles. The data was then sent to the National agency for secure documents (ANTS), which compared it using a facial recognition software. If there was a match, the agency issued the user with a personal code with which they could identify themselves on all public online services including FranceConnect via Alicem.

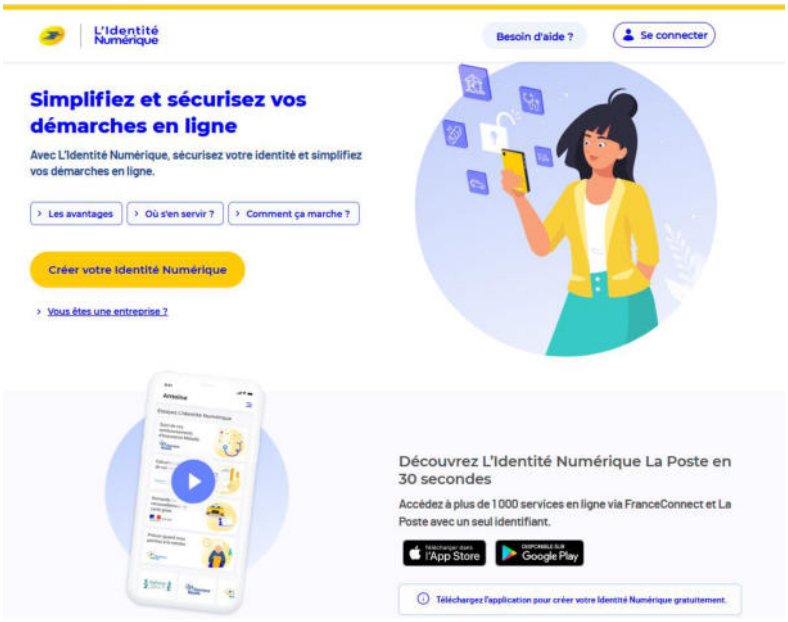


Figure 8 La Poste eID screenshot

Source: Bertille Auvray

Figure 9 La Poste eID screenshot

Source: Bertille Auvray

eID systems using facial recognition seem to have a difficult stand in France. In 2019, the French government was the first European country to introduce an eID system using automated facial recognition. The launch of the ALICEM-system ("Authentification en ligne certifiée sur mobile") was accompanied by massive criticism from data protectionists, IT security experts and civil rights activists. The ALICEM-system, which was developed by Thales´owned company Gemalto, used the information stored on the chip inside the old French passport which was to be scanned by the user with his or her mobile phone. The passport ID information was combined with a video selfie which the user needed to shoot in which he or she had to film himself or herself from different angles. The data was then sent to the National agency for secure documents (ANTS), which compared it using a facial recognition software. If there was a match, the agency issued the user with a personal code with which they could identify themselves on all public online services including FranceConnect via Alicem.

Data protectionists pointed out that the system required only a simple - and weak - password to create the user account and criticized the necessary security. Also, the fact that facial recognition was being used was compared with the situation in China and was generally rejected by French data protection activists and parts of the population. In 2020, the ALICEM-system was discontinued. The new CNILe/ SGIN-system does not use facial recognition as a mode of identification, although it also uses biometric information stored on the chip of the new ID card. The advantage of the new CNILe/ SGIN is that users can generate electronic certificates comprising only the identity attributes which he or she considers necessary to transmit to third parties of his or her choice, officials said when presenting the new system in 2022 (Phillips 2022).

Banks use a two-factor authentication (under the Payment Services Directive 2, PSD2) i.e. authentication with a personal key plus password, then a second secret code to validate any transaction.

Concerning facial recognition: “Blablacar”, a car-sharing application, uses a principle similar to IMPULSE to match the identity document (in this case a driving licence) with the face thanks to a selfie to validate the identity plus the possession of a valid driving licence and use the services.

Sources

- Balian, Christine (2021): The French eID ecosystem FranceConnect. Webinar Worldbank, September 22, 2021, www.worldbank.org/content/dam/photos/1440x600/2022/feb/FranceConnect-world-bank-webinar-20210927.pdf
- Elina S. (2023): “France Identité : tout savoir sur l’appli d’identité numérique et ses dangers”, In: LeBigData magazine, March https://www.lebigdata.fr/france-identite, March
- European Commission; Deloitte (2021): Overview of Member States’ eID strategies. CEF eID SMO Version 3.0, January 2021. Authors: Massimo Pedroli, George O’Neill, Arianna Fravolini et al.
- Gupta, Deepak (2021): FranceConnect +: what you need to know about this evolution of FranceConnect. In: Techunwrapped.com, September 15, 2021, https://techunwrapped.com/franceconnect-what-you-need-to-know-about-this-evolution-of-franceconnect
- Phillips, Tom (2022): France to let citizens generate digital ID by scanning physical eID card with NFC smartphone. In: NFCW.com, May 4, https://www.nfcw.com/2022/05/04/377038/france-to-let-citizens-generate-digital-id-by-scanning-physical-eid-card-with-nfc-smartphone/

List of participants

Participant No.	Organisation
1	Idhetic company for a decentralised digital identity portfolio for all users
2	Support to entrepreneurs and small companies on issues of accessibility and implementation of advanced technologies, especially with AI. Development of technology to support their growth and sustainability. Observation of the delay of European solutions compared to the USA. And also question of RGPD.
3	Work on integrative solution to be proposed to each user to make them more autonomous (approach, data management, etc.).
4	eflection on how to decentralise what is currently still too centralised (particularly identity) in the private domain and do this in a private manner and avoid over-exploitation of user data (e.g. for the purchase of alcohol, we ask for +18 years, but we also recover a lot more unnecessary data).
5	(trusted AI and ethics for EDIH DIHNAMIC) risk associated with the use of AI in certain areas = date cycle, trusted AI, GDPR. How AI applies to certain number of technical nodes.

6	Eiffage énergie système (private), intervention on a project at the end of deployment for the installation of a biometric identification terminal (digital fingerprint) for access control on an industrial site (nuclear power plant).
7	Project manager at Keeex, a specialist in the use of blockchains, with technology that allows any type of file format and process to be protected and made verifiable.
8	Works at FIM (laboratory for the evaluation of secure electronic transactions, in particular on biometrics).
9	In charge of intelligent territory and open date at the Rouen Normandy metropolis.
10	Intelligent territory referent at the agglomeration community
11	Former manager in a Bank
12	Digital trainer at the Red Cross (interest in the issue of digital identity for the general public and for employees).
13	Consultant in digital transformation, working with private and public players who have questions about authentication (dematerialisation of procedures, signatures). Also working on digital identity.
14	Notary in a rural SME, mainly using dematerialisation of documents and electronic signature on a daily basis.

Table 11 Participants in the French workshop

A.4 Documentation of the Nordic countries workshop on March 2, 2023

Title of the workshop:

Smartphone based digital identities using facial recognition for public services in the Nordic countries. IMPULSE solution, use cases, adoption requirements.

Who was in the workshop?

Hosts of the Nordic countries workshop were the IMPULSE project partners from Denmark (ARH), Finland (LUT) and Iceland (RVK). Also, project partners from Cyberethicslab and Grandiant were present to answer questions concerning regulation and technology. The workshop registration was done via the Fraunhofer website.

The language of the workshop was English and in the break-out session dealing with the situation in Denmark, the language was Danish.

The workshop was held online on March 2, 2023 from 10 to 11:30 o´clock. 24 external experts and 12 persons from IMPULSE participated in the workshop. Most of the external experts came from Denmark, second in numbers were experts from Iceland, and third was Finland. The Islandic and Finnish experts formed a joint break-out group.

Because of the different time zones the three countries were in, the workshop had three different starting times: 9 a.m. in Iceland, 10 a.m. in Denmark (CET), and 11 a.m. in Finland.

The 1,5h-online workshop had the following agenda:

- Overview of the IMPULSE solution, including use cases (in English) by Nicholas Martin (Fraunhofer ISI) (20 min)
- Questions and answers (10 min)
- Two break-out sessions:

  Group 1: Denmark (in Danish)
  Group 2: Iceland and Finland (in English)
- End of workshop at 11:30 CET

The slides used for the presentation can be found in Annex B.

Questions and answers following the presentation of the IMPULSE solution

Question: How much are **possible cyber attacks** dealt with in the project? I ask because of the current crisis that we have in Europe. We will see more and more cyber attacks. How is this covered in the IMPULSE project? Also, I would like to know about the possibility of carrying out **digital elections** with the solution.

Answer: Both aspects are interlinked. When it comes to elections, we really have two basic security or integrity problems of vulnerabilities. The first is, is it really you who is logging in and the second is that nobody is afterwards **hacking into the system to manipulate it**. The first point is addressed in the IMPULSE project and the second is also taken care of. Details were given on the technical aspects concerning the **security aspects of the system.**

Concerning the security question, the main focus of IMPULSE is to ensure that the execution of the cryptographic operations of the solution are trusted. So our main focus is to execute trusted execution environments in both the enterprise world, which is the one used by the public administration and the user wallet which is the user application.

New smartphones usually have some cryptographic chips that allows to execute and store cryptographic keys in a secure manner. We are planning to use them. And for the public administrations, there are trusted execution servers that allow to safely store and execute cryptographic operations, and that's our main concern, because

the whole system relies on that private keys remain private and the user can be the only one to sign a verifiable credential and present it.

Question: Authentication by taking a new selfie. **Is there any assurance that this is actually a life selfie and current selfie and not just an old picture**?

Answer: We have included filters to know that it is a life selfie. It has to be take for about two seconds and we are able to say that the selfie has a liveness.

Question: **How do you handle false negatives**? Using fingerprints on Android phones requires to re-enrol at some times because fingerprints change a little and the same goes with the facial recognition. These change could lead to false negatives. You don't want to enrol people wrongly, but you also **don't want to reject people** because then people consider the system useless. So how you handle this?

Answer: Facial recognition has in general less false positives than with fingerprints. And we keep evaluated every few months and then add new filters continuously and the rates are improving. But in fact this could be a problem when scaling up the system.

Remark: Are you are using the task camera on iOS? I don´t think so because you won´t have access to that unless you use face ID. Using a video selfie could currently help against **deep fake technology.** But it´s a battle between cat and mouse. Deep fakes are getting better with time. How do you envision that?

Question: Will the IMPULSE solution have the possibility of **handling authenticating requests from users from all over the world or are you focussing on specific formats of ID cards?** Because for us in Iceland can like that's the main challenge. Like we we have really good coverage with this like these. But for some digital services we need to be able to service foreigners and our solution is too limited, being only European and so we have been looking into other options to support this, including biometric identifications. But then you need a system that understands formats from all over the world.

Answer: We've been developing the system based on a the IDs of the five involved countries with use cases in the project. In the longer term, of course, there's of interest and the intention is to be integrating more.

Question: Could you clarify how the **automatic versus manual verification** works?

Answer: Refers to the animated video we sent around and describes the details of the authentication process. And then there is still a manual check of a real person in the back-end because that is what the law requires. This is of course a challenge when scaling up the system. But that is a challenge that that currently all systems are in due to **European legislation** at present.

And going forward one will have to see - depending how the technology and how the threat environments develop - to what extent this continues to be necessary and also to what extent does this really help to combat threats. But I think that's a a longer term discussion.

Documentation of the break-out sessions

Group 1: The Denmark session

The purpose of the Danish breakout session originally was to explore topics around possible benefits of having multiple available eID solutions in a Danish context as well as possible benefits of biometric identification and login. It was planned to last one hour. However, as the Q&A-session took longer than planned, the break-out session was shortened accordingly. The remaining time was used to give each participant the opportunity to come up with her/his view and thoughts on the IMPULSE solution and the Danish use case.

Participants of the Danish break-out session found it interesting to hear about the project. Most of them wanted to be kept posted about the development of the project. The main reasons for wanting to engage in the workshop and hear about the project was due to:

- Interest in the landscape of digital signatures and eID's
- Interest in the question of the need for multiple eID solutions in Denmark
- Interest in the development of eID's

- Interest in the relation of the IMPULSE solution to the EU Digital Wallet
- Interest in biometric identification
- Interest in facial recognition issues like head injuries, wounds, colour etc. and how the IMPULSE solution addresses these issues
- Interest in digital inclusion in self-service solutions

In the beginning, the Aarhus pilot was presented in more detail. the Danish IMPULSE-partner explained that the reason to participate in the project is because it deals with possibilities for a **common European digital identity solution** and we think it is important to be able to influence this in the early phases – this is one of the very first pilots in this area that deals with some of the new policies and programs in the EU regarding digital identification.

We think it is interesting to go from a centralised architecture in this area to a decentralised architecture. We also think it is super interesting that you will have more ownership of your own information with this solution than the case is today. That's where we are coming from.

We chose the case with vulnerable citizens because we want to test the facial recognition in context of a shelter. Because if it works in this context there is a good likeliness that we will be able to implement the solution without many difficulties in a whole population. We are interested in the answer to the questions: Can you be so "high", that you can't use facial recognition technology, or can you be so badly hurt, that you get rejected by the app.

Comment from FinansDanmark (a bank): We were heavily involved in the development of MitID in corporation with Digitaliseringsstyrelsen [the Danish agency for digitalization], so therefore we are, of course, naturally interested in digital signatures and means of digital identification. We are also participating in a work group in relation to **the new EU Wallet**, which is in its early stages at the moment, but will develop into a transnational solution both for identification and hopefully also for approving transactions, like e.g. payments. That has our interest. Thank you.

Comment from Sundhedsdatastyrelsen [the Danish agency for health data]: My question is **how stable is this technology** if users sustain an injury? Will they then be rejected? In the field of healthcare, we see a lot of people that get operated, get wounds and things like that – and that is important to be able to handle. And then there is, of course, some considerations about whether it's a good idea to **have multiple competing identification solutions**, or if that just creates more confusion among the citizens in Denmark, who already thinks its complex.

Remark from ATP [the largest pension fund in Denmark]: I'm working with the Single Digital Gateway at the moment and I'm going to look at the **EU Wallet** and how these are linked. So, I'm participating today to find out how this project is linked to the European Wallet and the integration we are currently working on – to get the member states **to recognise each other's IDs, so it's possible to move across borders** – without having to - when you come to Denmark - then you don't have to acquire MitID, you can continue using your Spanish ID to get along. We are working a lot with the EU eIDAS regulation, and we are interested in how this project is linked, and also the question of why we need multiple eIDs.

Comment from the Region Midtjylland [Central Denmark Region]: The reason why I think IMPULSE is relevant is because we, The issue of secondary data is important. We as the Region Midtjylland are collaborating with Sundhedsdatastyrelsen and affiliated partners on a 'Proof of Concept' for secondary data sharing. We also collaborate in the joint action in EHDS to get primary data moved across borders, where data from different agencies are in play on the health domain. At the moment we are the only Danish region who works with Sundhedsdatastyrelsen on getting all the regions to begin creating the infrastructure needed. So, that's our interests in this area.

Comment from the ULF [national association of the developmentally disabled]: We represent 10,000 members with **developmental disabilities**. Our members are rather overrepresented in the group – estimated at between 7% to 22% - that has problems with digital solutions. That is, not only problems with them being annoying to use, but problems with actually being able to use them. And I'm very excited to be here, because our own members really want – well, you could say, something easier. We see a **big potential in facial recognition** – in regard to not being made unnecessarily unable to handle your own affairs, as some people experience now

- because for some people MitID is a somewhat positive development, but for our members, it was a very negative development. It has made it much harder for them to handle everyday stuff like money, and so on.

An expert from the Institute of Humans and Technology at Roskilde University explains: The case with the shelters is a really good use case. Also, I have a comment about having one or more ID solutions – the important thing is, that each citizen can choose what is best for them – then we, as a society, have to offer different ways of access.

This comes down to the central issue – the first registration, the first identity we get – the analogue identity we get at birth – and how we get registered then. And then we had that big problem, when the banks stopped accepting NemID [the precursor to MitID], then Citizen Service suddenly had to do manual registrations for those who didn't have the right passport or enough trust – now all of that is finished.

Some of us didn't have to show our passports, apparently, because we were registered in the financial institutes so recently, that we didn't have to show our passports again. But specifically with this solution, you don't use passports, but you still have to do manual registrations. That was the clever thing about MitID, the registration process. Those who already had been manually registered, they were able to data chain through a chain of trust, and then register with their old ID to get the new ID. That, I think, is an important element, when you think about these and when you have to implement these, that you are able to do that, because that's what is going to get the solution implemented.

It's also interesting having a decentralised architecture, but fundamentally, then I think, from experience looking at registration processes, then we get back to how we get registered in the first system, and there are some grave weaknesses, that we in Denmark actually don't know about who is whom – and it is not just the municipalities, its centrally with the CPR-registry [the central registry of people in Denmark] and how we get registered there - there is no check on people. Its fortunate that we have a society with a high degree of trust, because otherwise this couldn't function.

Comment from the Council of Socially Vulnerable: The Council is generally interested in the digitalization agenda, and in regard to the fact that people who are socially vulnerable often meet the public system and needs to be guided by the supporting systems, whether talking about the social domain, the employment domain, the housing domain, the health domain – in all kinds of situations there are digital self-service solutions with the possibilities and barriers that entails for these people - who often live chaotic lives, which we heard something about in the introduction to the Aarhus-case.

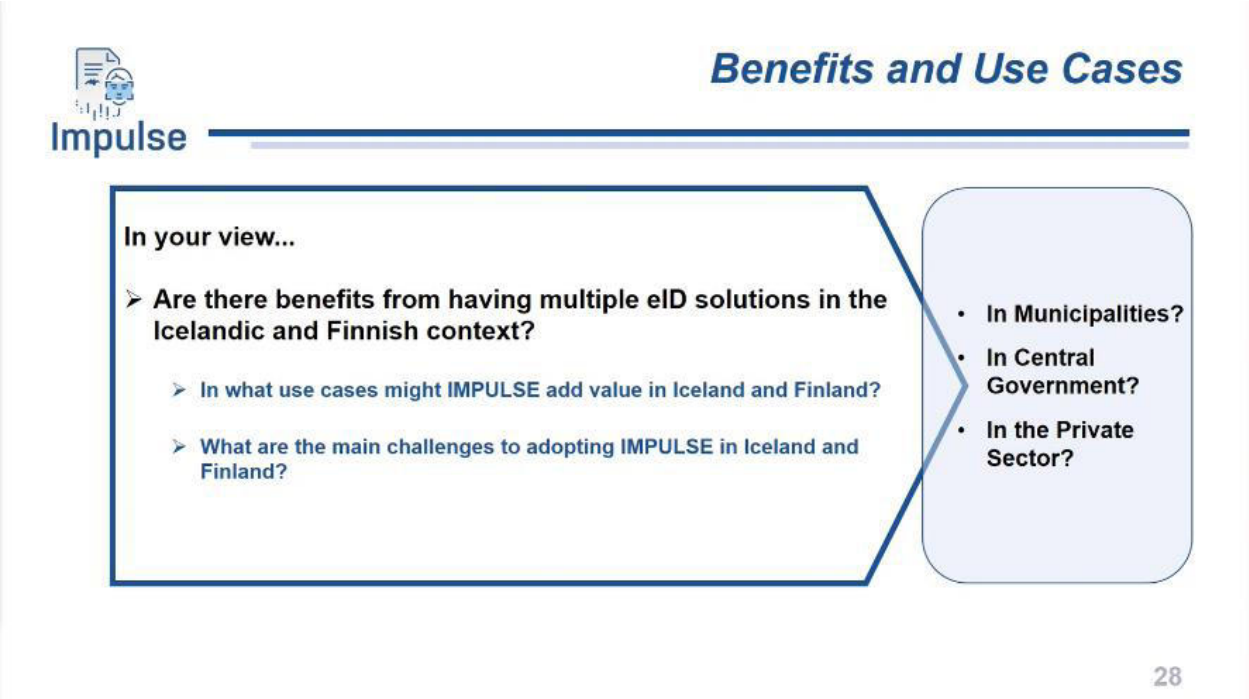
Comment from the Digital Lead [Denmark's cluster-organisation]: We have a broad network of interested parties in this ecosystem. Personally, I think this case is interesting, since it touches the current agenda in digitalisation politics, where our new minister of digitalisation, Marie Bjerre, also is focussing on digital inclusion from different perspectives, and that is what this technology is trying to address. This challenge has arisen as our society has become so thoroughly digitalised, that it has become very complex. So that is the perspective I find interesting regarding digitalisation politics.

I agree with things coming from Sundhedsdatastyrelsen and ATP – you will probably have to handle this projects relation to the EU Wallet – how many identity channels do we need? – even though, I know, **we both have a passport, a driver's license and so on in the analogue world.** I think this is something you need to consider, to risk-assess in some way. Like when we have different public mailboxes – this is a bit different – but that can also make it hard to handle - "where do I get my mail, is it in the blue, green or red mailbox that my mail from ATP is?". (I know, they don't have these colours, it's just that there are actually three public mailboxes at the moment.)

Comment of the Danish IMPULSE-partner: A big part of this project is the handling of interactions and overlaps with EU-programs and new regulations in this area – an Italian partner in IMPULSE is responsible for this and shares information with the other programs in progress.

Comment from Sundhedsdatastyrelsen: I'm working in the Decentral Cyber- and Information Security Unit in the Health Sector, what called DCISsund, and we are interested in both the security aspects – and I agree much what was being said especially on the finding that systems need to work across data silos, both for primary and secondary use of health data. There are some activities in the EU in order to find a way **to share health data** and, I think, there will be some forms of identification issues to address.

Group 2: The Iceland and Finland session



Iceland and Finland have quite developed digital identity systems so my question here is, do you see any benefits in having an additional identity system based on the IMPULSE model, available in Iceland? Or would you say, given the range of systems already available in Iceland, this is not really an issue?

Comment: From my personal view, Iceland is a small nation, and we must be very mindful of where we spend our limited resources and efforts. We already have good systems in place. They are centralised yes, but they have been evolving and there have been new products in the market and the expert from Auðkenni[6] can talk more about that.

I believe the main thing is that we have been actively **moving from the password systems, replacing them with electronic IDs** as well as registries, for example, for companies or for managing your children – an authorisation system around that.

The main challenge remaining for us are people who have difficulty obtaining or using electronic IDs, for example, we are already working with **disabled people**, and we have a management system in place, but there are also small subsets of the population that do not use electronic IDs. I am not sure if the IMPULSE solution would be a better alternative for those parts of the population. Then another challenge I see are people who are moving to Iceland or do business in Iceland, and this is something we have been discussing more recently and why I was asking earlier about that in the main session. But it sounds like IMPULSE is not there yet –not the focus.

Question: IMPULSE is funded by the European Commission, in this case centred on policy developments regarding the future of European-wide applicability of eIDs. My question to you Icelandic experts. I am still curious to know how far we are in Iceland thinking ahead. Will the technical protocols we have today **become obsolete shortly or will they be compatible with eIDAS2** for instance? Perhaps this is very self-centred on European development but that is where we are with our commitments to the internal market.

Answer of Iceland IMPULSE-partner: eIDAS has not been a priority for us in the project. We want to look ahead, and we have been looking into e.g., Mobile Travel Licence (MBL) which is not the same as eIDAS but the principle [cross-border inter-operability] is related. The business environment is where we are looking ahead mainly but the technical solutions are not quite there yet.

Question: Can you explain for which market the IMPULSE solution is being developed for?

Answer: The bottom line is that across Europe you have a very uneven landscape regarding how advanced countries are in using digital identities. Some places like Iceland, the Nordic countries, the Baltic states and

[6] Auðkenni is the primary trust service in Iceland, majority owned by the Icelandic state.

Belgium for example, are very **far advanced with one or two eID systems very broadly used** already. Then you have other countries, be it Germany or Spain or Bulgaria which are **behind, where either you have highly fragmented systems**, like a plethora of small-scale solutions developed by various companies or service providers, not in broad use – or, in some places there is not very much at all in place, maybe one or two small providers.

So, the broader challenge when looking at these countries is very much what IMPULSE is about: 1. **Developing a widely used solution** with which to enable various forms of digital government and digital economy and, 2. Achieving a degree **of interoperability between these systems [countries**] so precisely that, say, if I move from Spain to Italy, I can basically onboard my Spanish eID over there.

Question: What could a system like IMPULSE bring to the identity environment in Iceland or Finland? Does it add something and, if so, what might that be?

Answer: Working as a product owner at the Digital Iceland project office which is leading the charge in central government digital transformation I would like to comment: The focus in central government – with limited resources – is **reaching out to those who are currently unable or find it difficult to use the existing eID**, and **reaching out to those who are seeking public services but are not residents of Iceland**, hence, unable to obtain the Icelandic eID. They still need to access certain services without that eID so perhaps IMPULSE can bring alternative solution to the table where we are unable today to provide access.

Question: What do you experience as the greatest challenges with equipping these parts of the population who currently do not have an eID?

Answer: The biggest challenge is the *physical elements*. You need to be physically present in Iceland and at the relevant site, setting up the eID and a pin number [e.g., at a phone company or the Auðkenni office] when obtaining the Icelandic eID. This is a challenge for everyone living abroad. Also, those who do not have the required Icelandic phone numbers cannot obtain the eID.

In terms of people with disabilities, they might be unable to obtain the eID as it is set up or not able to remember their pin number. That is a big challenge but, as someone mentioned in the main session, if a person is unable to obtain and use an eID, how equipped are they to use the online services accessed with that kind of authentication? The challenge is then also about **simplifications towards more inclusive accessibility** of online service systems (ease-of-use) as much as it is about overcoming hurdles with the eID. So, these are the two greatest challenges now, but that can change in the future.

Comment: One of the things that IMPULSE does is to involve manual input from service staff in the registration [onboarding] process to verify identity so that from the user's perspective, the onboarding and use of the IMPULSE eID can be done from the sofa.

Comment: Being the CEO of Auðkenni, the main eID provider in Iceland and having been in the eID business ever since attending an EU eID expert group meeting in 2005 I would like to comment on the question whether there is space for the IMPULSE solution. We have been building the eID infrastructure in Iceland since 2005 and we now have the wide distribution, so **it takes a long time to build up these kinds of infrastructures**.

And, it is **not just only about the technology. It is a lot about the clients and standards, regulations and rules** and other aspects that need to be considered.

Apart from the infrastructural developments in Iceland, we have been working on biometric solutions to add into the mix. We can say that these solutions are addressing the same or similar issues that IMPULSE is also addressing, for example, not needing to be physically presented during registration [onboarding]. So, we have an app where we are adding a biometric onboarding possibility with a selfie and comparing that with an ID. The difference, compared with IMPULSE is that we require the user to have a phone with NFC capability, so we collect the information directly from the chip of the passports. In other words, we don't allow capturing a picture of the physical ID. So, that is an even more rigid requirement. There are so many aspects to this, we produce false positives and negatives and we are working with the strictest requirements on the likelihood of positive verifiability of the person the ID belongs to. This means that for some people, we lock them out of the system when the algorithm suggests, no, I'm not sure it's you.

So, all these solutions can be applied in different ways, it just depends on how secure they are and, one of the biggest problems in new systems like this **is not the technology, it's the compliance, it's the business model,**

business responsibility, who is liable, what happens if there are mistakes, is it the service provider, the technology vendor, who is responsible for fraud?

When I first came onto this scene in 2005, I thought this was really simple but, within the EU context, **issues of liability** were heavily debated across countries and within them. For example, this biometrics solution that we are adding on, being a qualified and certified trust service provider, we are selecting a solution and vendors that are certified by eIDAS and we are working with another qualified trust service provider and it has taken us now half a year to a year just to go through the **auditing processes of implementing** and we are still in the process of Icelandic regulators and supervisory bodies reviewing so, only that part takes a huge amount of time while the technology has been ready for a while. Just the auditing part takes a huge time and every time you change something you have to go through the process again so, those are the rigid requirements that come from the regulation and from eIDAS and we can be very underestimated in all of this, and it makes it also more difficult to adjust to changes elsewhere, for example, when someone like Google or Apple change something – since we interoperate with their technologies as all.

Also, how many choices can we have? We are now working towards eIDAS2. The EU is proposing a legislation that is still under review and hasn't been implemented but we are participating in **large scale pilot** where we are using **eID wallet**. So, what is the relevance of the eID wallet in the context of the IMPULSE project? What I mean, there are many cases [out there] and service providers like municipalities, governments or banks cannot accept huge amounts of different solutions. It is difficult to get agencies to accept new solutions we offer. Auðkenni is working with all the online service providers, but we are adding a new app, a new way of authenticating and it is taking a long time to implement that with all those service providers. So, **we have a great solution, but the difficulty is to get someone to onboard** onto it and the service providers to accept it in their communications.

Question: Can I ask you to go a little bit more into the regulatory and compliance side from your experience and what you see as the most important requirement and the most important hurdles or where do things become really difficult.

Answer: Well, this is nitty gritty stuff, for example the eIDAS regulation and you have ETSI standards, different standards and there you have a thousand boxes to tick and that is complex. Then you have those grey areas with these solutions where you are judging how well they adhere to this and that, and then we have certification bodies that are vetted by the EU so, this just takes a lot of time.

The technology is moving so fast and if your solutions require certifications and vetting, then the technology moves, and you lose the certification and then you need to move on and catch up and this can be so difficult and expensive as well. So, how to keep up?

Also, this is about **security vs. usability**. The higher the security requirements – barring false positives – you exclude people. The requirements become too rigid for some people to use the technology. Then, if you look at different groups of users, eIDAS regulation has requirements that exclude certain kinds of people, e.g., the directive of 'sole control'.[7] So, if the user does not have sole control, they are excluded from solutions that fulfil this requirement. Then you need other solutions, and we talk of mandates and the EU has been addressing some of the difficulties. We will have different solutions for different scenarios. It is difficult to have one for all. We can have one or a few for most. Then you have the niches and how to address them then in different ways.

Question: What level of assurance is IMPULSE targeting? Have you been looking into certifications for the authentication using a selfie? The Icelandic solution using the selfie, is that going to have high assurance?

Answer: It depends, you have different assurance measures, ISO standards, the eIDAS regulation raising the bar high. In Iceland, we are going to be issuing a technology that has been used, e.g., in Estonia for a few years now with qualified signatures. But, there is huge difference between **taking a picture of an ID and using the NFC capability**, accessing directly the information on the chip which is authentic and can be checked so there

[7] The directive dictates that the user is in sole control of her/his qualified signing key for authorisation with no one else having access. The eIDAS regulation has repealed the directive and explicitly relaxes its sole control requirements in a trade-off between security and usability.

is **huge difference in terms of security.** But, here you exclude as well because users need to have devices that are compatible and we may have NFC issues, so on and so forth. Then we have within Europe different solutions that are not as secure, deemed to have the same level of assurance which is dubious.

Question: Does the selfie verification in the Icelandic biometric system have a manual component?

Answer: It is a automated process, using algorithm.

Question: I am not sure if Xavier picked up on the question earlier in the context of IMPULSE. In our recent project meeting in Madrid it crystallised that you have to think in very different ways about services or identity providers and authentication in use cases where there is an **absolute requirement that you have to prove that you are indeed the person you say you are**, and then ALL the other cases where it doesn't really matter. You can create all sorts of bogus identities to use all sorts of online services and it doesn't involve serious risks. That distinction suddenly crystallised with the realisation that the technology developed within IMPULSE has not reached the maturity of breaking into the market, say, to become an alternative option on http://island.is. It would have to reach certain maturity and go through the different auditing processes, and I wanted to ask what it means if eIDAS2 will come into force in 2023 or 2024?

Answer: eIDAS2 has not been passed by the EU, it is still going through review processes, but we started pilots that are testing the technology and the infrastructure that is being proposed in the legislation. We are ahead of ourselves but the biggest thing in relation to this aspect – the eIDs inserted into an eID wallet will come from centralised IDs [referring to centralised registries of residents]. This has been debated since I came onto the scene in 2005, why can we not do the same as with passports, centralised IDs within Europe? Then you have the Germans saying that they can do it but only in their own system, and the Austrians do one thing and the Spanish go with them, and so on.

One of the most complex things is not the technology but **how to set up a unique identifier like we have in the Nordic countries**. We have personal identifiers we use with everything. How do you do that within the EU/EEA? We have countries that don't use unique identifiers so that is one the complexities in all of this – to deal with that. But, the eID is something that the EU is pushing for – a new European identity solution which will take over in all the included countries and then will be difficult for other solutions to have space. For us, we have the eID wallet and are going along with this legislation (eIDAS2), we implement that in Iceland, then we have something from IMPULSE. Should we be focusing on that or the eID wallet?

Question: The EU seems to be pushing the eID wallet and eIDAS2 regulation so what I'm thinking is what is the relevance of IMPULSE? Does it go hand in hand or are these competing solutions?

Answer: I think I can clarify that quickly. IMPULSE is one of those technology development projects that are following what is promoted in these areas of development by the Commission.

Question: Does it work with eIDAS then and the eID wallet?

Answer: I think the latest specification of the EU **eID wallet** was released some weeks ago but, as far as we know, IMPULSE has been piloted in the EBSI network which has an identity model, eSSIF [European Self Sovereign Identity Framework], also supported by the European Commission and, as far as we know, EBSI is trying to be compliant with the EU eID wallet specifications so we [IMPULSE] should be able to be compliant and interoperable with them [those system specifications] and not be competing as some substitution but, we are in early stages and the eID wallet is just a specification for now.

To be clear – this was probably obvious – but the IMPULSE system involves a wallet functionality.

Question: So, the drive towards all these large-scale pilots now across Europe, the EC is funding, is IMPULSE **involved in any of these large-scale pilots**?

Answer: I believe not. We have our own pilots that we are doing as part of the project and we are in exchange with other projects but, to my knowledge, our pilots are not part of these large-scale pilots. The IMPULSE

project was basically conceived back in 2019-2020 and then received the funding from late 2020 onward so that may have been a little bit beforehand.

Question: Going back to the question of the **selfies** and what people use it [the technology] for. The research that Fraunhofer and I am doing for this project is focused in terms of how people react to these technologies, to what extent they accept them or not, and also what impacts they then have. One of the things we are doing is a large-scale survey and one point that we are interested in, is for what sorts of applications or use cases do people think this [IMPULSE] could be a suitable solution. One might think that a selfie and biometric information is all quite sensitive information so maybe people only want to use that for particularly sensitive and high-value services, for instance, banking or health, while more conventional services like social media are not so sensitive and people would not particularly want to share biometric information in any shape or form with the service providers.

We are in the state of collecting the data so, this is early analysis looking into them and playing around with them and, interestingly, the people we are surveying do not seem to draw a **distinction between authentication and service access**. When they are interested in using these (authentication] systems, they become interested in using biometric logins for all manner of services.

Background report: Denmark

The Danish national eID is called „MitID“, it can be used for e-government-services, online banking and other business services as well as e-health-services. Predecessor of MitID was NemID, an electronic ID system that used paper TANs for authentication and which was in place until June 2023. At the time of the switch from NemID to MitID in 2023, more than 90 percent of Danish citizens have their own national eID, be it as a PC and TAN or as a mobile version where the initial verification is being done via NFC using the chip of the Danish ID card and the identification for individual services via a mobile TAN.

The basis for the Danish eID is the central personal identification number, the CPR number ("Centrale Personregister"), which has existed in Denmark since 1968. This number is used by practically all Danish authorities and also in the healthcare system. The number helps to avoid confusion, enables offices to process applications automatically, and allows public administrations to exchange data with each other. In 2010, the government transferred the CPR number to the Internet: It introduced a digital identity called „NemID“, which citizens use to log on to government websites and sign documents digitally. The NemID infrastructure was developed and operated by a private company, the financial services provider Nets. From the outset, Danish banks also used NemID, so the service quickly gained widespread acceptance among the population. One of the reasons was, that the government made the use of numerous online forms mandatory for citizens, so that Danish who wanted to use the services had to apply for a NemID (see Wölert 2022). But also the fact that it could be used for online banking and other services as well made the eID attractive for Danish citizens.

According to consulting firm Arkwright, the initiative for a joint eID (for e-government and e-banking) even came from the banks: „The Danish Bankers Association initiated preliminary discussions with the Danish government to form a joint e-ID in the early 2000s. The usage rate of 1-2 times a year for the public e-ID was low, (citizens often couldn’t even remember their login data) so the government saw great potential in a joint e-ID. The main driver for banks to collaborate was again the security aspect. The cooperation of not only banks, but also authorities was mainly the result of extensive cost sharing possibilities. The provider Nets, majority owned by Danish banks, was chosen to operate the 2010 launch of NemID, Denmark’s national electronic ID and digital signature infrastructure based on PKI technology“ (Arkwright 2019, p. 26).

With the MitID, the new version of NemID, Danish citizens can use for example the following e-government services, which are accessible via centralized in the website www.borger.dk:

- change of address
- application for childcare
- reimbursement of taxes
- selection of a doctor

- use a personal digital inbox (source: https://lifeindenmark.borger.dk/apps-and-digital-services/nemid)

The MitID system offers all three levels of assurance (LoA) from eIDAS, Low, Substantial and High: „Low“ authenticates the user with single-factor authentication, e.g. with password or chip, „Substantial“ authenticates the user with a two-factor authenticator combination, e.g. with the MitID app on a smart phone and „High“ authenticates the user with a more advanced two-factor authenticator combination, e.g. the MitID app plus chip (see Signicat Developer 2023).

To get an MitID, Danish citizens can scan their passport using the MitID app (see figure 1) or they can go to a Citizen Service (borgerservice) office in person which requires an appointment.

If the service requires extra security - for example when transferring money through online banking – MitID-users have to enter a PIN code or approve with facial recognition or fingerprint.

eHealth: The yellow health card (Sundhedskortet) is required in Denmark to receive medical treatment. There is also a digital version of the yellow health card, the app is fully valid and citizens do not need a physical yellow health card if you have the app. The yellow health card needs to be shown at the doctor´s office as well as at municipal offices. It is also required to receive a NemID. It can also be used at libraries, for identification in post offices and stores and in many other situations.

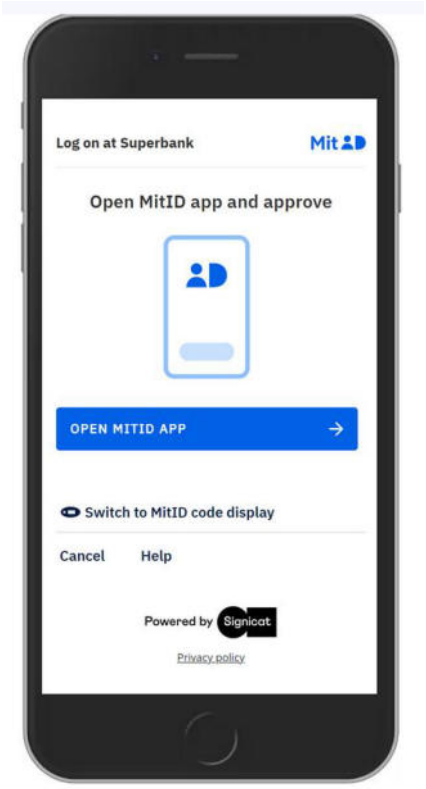


Figure 10 Mobile login with the Danish citizen eID „MitID“.

Source: Signicat Developer 2023

Sundhed.dk is the official portal for the public Danish Healthcare Services and enables citizens and healthcare professionals to find information and communicate. The portal facilitates patient-cantered digital services that provide access to and information about the Danish healthcare services. Citizens can log into the portal using their Nem ID/ Mit ID.

Background report: Iceland

Citizens in Iceland can use the country´s mobile eID for e-government services, online banking, and other business purposes. The introduction of the mobile eID in Iceland was described as a „good practice“ in the 2022-EU-report „eGovernment Benchmark“ (European Commission 2022). According to this description, „Ísland.is has released an app to bring better public service delivery in Iceland. The first version of the app gives direct access to a digital mailbox and public certificates, such as drivers' licences. All institutions in Iceland must share data through the digital mailbox by the year 2025 and the app simplifies communication with the public. The app shows the status of applications with institutions using the new application system at Ísland.is, bringing more transparency for applicants. The driver's licence overview gives the user access to the details of their driver's licence. It is a quick, convenient way to obtain an official digital driver's licence that can be stored and displayed in a mobile phone wallet app“ (European Commission 2022, p. 23).

To get an Icelandic electronic ID, citizens need to bring their passport and their kennitala (social security number) to one of the three main Icelandic banks (Arion, Bank of Iceland, Landsbankinn) or one of the offices of the country´s cell phone provider offices (Siminn or Vodafone), where their identity is being verified. Then, anytime they want to use an e-government service, open a bank account, buy a car insurance, etc. eID owners have the option to select to login with their eID. Then, a login prompt pops up on the smart phone to enter the smartphone number and the 6-8 digit eID-PIN. There is a national database cross-checking name, address, phone number, etc., so the person is known as soon as he or she logs in.

The eID is valid for 5 Years. Then the user need to go to one of the service points in order to extend the validity period. The eID is saved on the SIM of the smartphone.

Before the mobile solution was introduced, Iclanic citizens could use the eID with a PC and a smart card reader. The mobile solution was realized in 20213 by Finnish company Valimo Wireless (called „Valimo Mobile ID“). The ecosystem relies on PKI technology and digital certificate security. The user´s digital identity, in form of the private key, is stored on the secure element provided by mobile operators (the SIM). The certificates are issued by Audkenni, Iceland´s national certification authority, in connection with the registration process. The system works as a legally binding solution for all service providers integrating the system into their infrastructures (see Valimo 2014).

eHealth: The mobile eID can also be used to log into the health portal "Heilsuvera" which is the centralized web application that offers citizens secure, digital access to their own health information and eHealth services. The portal is integrated into the Icelandic Electronic Health Record (HER) and provides access to health information and eHealth services for citizens through this single access point. As health data are sensitive personal data, eID is the request for accessing the health portal. (source: National Centre for eHealth in Iceland 2021)

Background report: Finland

Finland´s eID situation used to be similar to the Danish situation with banks being the main driver and provider of electronic IDs which can also be used for e-government services. One difference is that in Finland, there used to be not not a single system in place but each bank has had their own authentication system. The different authentication systems were made compatible to each other, the interface combining all existing solutions was called „Tupas“ and was managed by a bank consortium. Establishing this kin d of system, citizens could use a single platform and at the same time, banks did not need to share their individual customer database.

However, in 2019 Tupas had to be terminated because of the European eIDAS regulation as there was no real real competition and the Tupas system was expensive for service providers and customers. The eIDAS regulation required the Finnish government to open up eID services to market competition. To that end, the government has established the Finnish Trust Network (FTN), a framework that allows strong authentication service brokers to resell eID solutions in Finland using a single standardised service contract (see Segnicat 2019).

Another authentication method for Finnish citizens is to use e-government services is to use FINeID, the government issued eID which is used in combination with the chip on the Finnish ID card. However, this

method is not widely used, the majority of Finns uses the eIDs of their individual banks (Arkwright 2019, p. 25). The national ID card is voluntary in Finland. It is issued by the Finnish police authorities and is valid for five years. Also, the Finnish eID card, which was issued in 2017 can also be combined with the Finnish Health Insurance Card. Finnish citizens have to go to one of 700 trusted retail outlets and delivery points for their eID/Health insurance card.

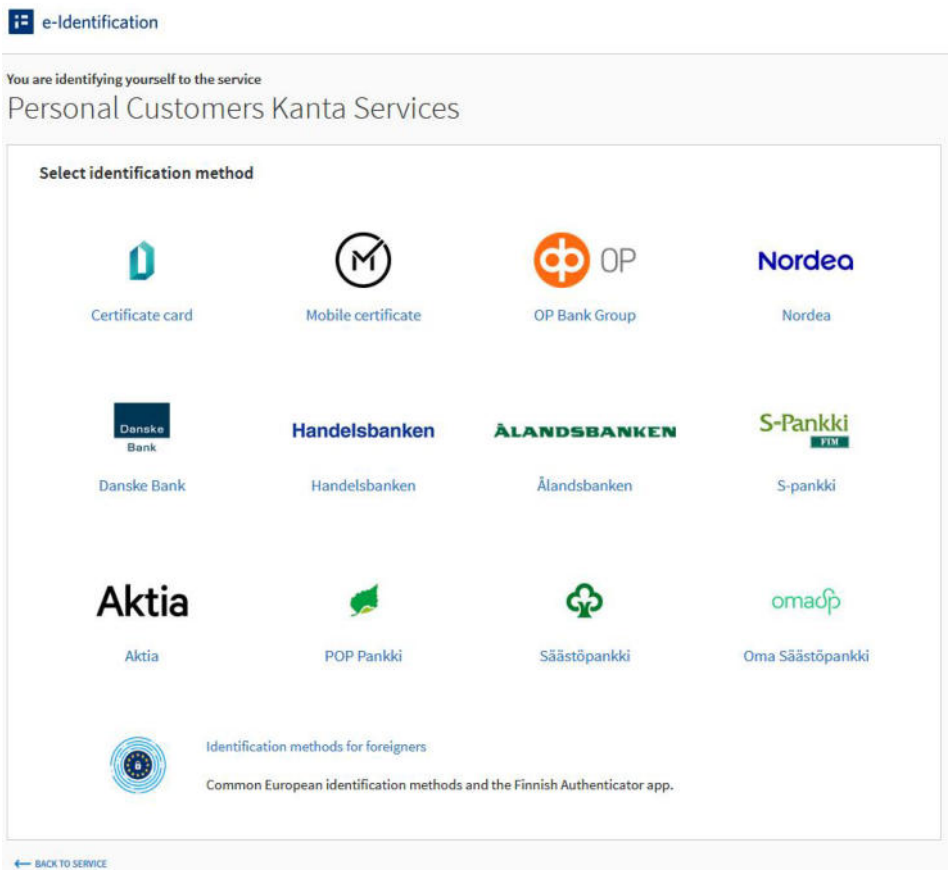


Figure 11 Log in to the Finnish e-health website Kanta

Source: https://www.kanta.fi/en/citizens

The Finnish government provides citizens access via the central public administration portal Suomi.fi

e-health: Patient documents are stored in electronic format in Finland. Health care professionals record the patient data in the Patient Data Repository maintained by Kela. This repository will in the future cover all health care service providers. The Kanta.fi service contains information on those health care units that are already recording their patient data in the Patient Data Repository. There are several options to log into the service (see figure 2).

Nordic electronic ID card

There are activities to introduce a Nordic electronic ID card which would work in Finland, Sweden, Denmark, Norway and Iceland. The proposal for the five-nation ID card was first recommended by the Nordic Council in 2017 and would fit with the long tradition of citizens in the region already being allowed to travel and reside in other Nordic countries. Denmark and Norway seem to be the forerunners concerning technological preparatory work for a Nordic electronic ID (see Vantinnen 2020).

Sources

- Arkwright (2019): Federated e-IDs as a value driver in the banking sector based on experience from Nordic markets. Authors: Eloïse Margrethe Langaker et al., https://resources.signicat.com/federated-eids-arkwright.

- Cruickshank, Alex (2019): Electronic ID in the Nordics – a model for other countries? In: Computerweekly.com, 14 May, www.computerweekly.com/news/252463291/Electronic-ID-in-the-Nordics-a-model-for-other-countries
- European Commission (2022): eGovernment Benchmark 2022. Synchronising Digital Governments, Background report. Written by Capgemini, Sogeti, IDC and Politecnico di Milano for DG Connect, Juli. Brussels.
- National Centre for eHealth in Iceland (2021): E-health services available for everyone and at all times in Iceland. Author: Gudrun Audur Hardardottir, www.healthcareatdistance.com/media/1121/e-health-services-available-for-everyone-and-at-all-times-in-iceland.pdf
- Valimo (2014): Moving from Citizen eID to Mobile eID. Case Iceland. https://issuu.com/valimowireless/docs/case_study_iceland_6_pp_folded_a5_w
- Signicat (2019): 7 things you need to know about TUPAS being replaced with Finnish Trust Network. www.signicat.com/blog/7-things-you-need-to-know-about-tupas-being-replaced-with-finnish-trust-network
- Signicat Developer (2023): MITID authentication process, April, https://developer.signicat.com/enterprise/identity-methods/mitid/authentication.html#normal-authentication
- Vantinnen, Pekka (2020): Nordic electronic ID card in the making. In: Euractiv, Jan 31, 2020, www.euractiv.com/section/all/short_news/helsinki-nordic-electronic-id-card-in-the-making/
- Wölbert, Christian (2022): Wie Dänemark zum Vorreiter bei der Digitalisierung wurde. In: heise.de, 18. April, www.heise.de/hintergrund/Wie-Daenemark-zum-Vorreiter-bei-der-Digitalisierung-wurde-6660933.html.

List of participants

The following external experts participated in the Nordics workshop:

Participant No.	Organisation	Country	Interest
1	Digitaliseringsstyrelsen	Denmark	Regulation & standards
2	ATP	Denmark	Regulation & standards
3	Region Midtjylland	Denmark	Regulation & standards
4	Roskilde Universitet	Denmark	Regulation & standards
5	Ældre Sagen	Denmark	Regulation & standards
6	Sundhedsdatastyrelsen	Denmark	Technology aspects
7	Central region of Denmark	Denmark	Technology aspects
8	Rådet for Socialt Udsatte	Denmark	Use cases
9	Aarhus University Hospital	Denmark	Use cases
10	Finans Danmark	Denmark	Use cases
11	Ældre Sagen	Denmark	Use cases
12	no affiliation given	Denmark	Use cases
13	no affiliation given	Denmark	Technology aspects

14	Finnish Federation for Communications and Teleinformatics FiCom	Finland	Regulation & standards
15	Haidion	Finland	Technology aspects
16	Taktikal	Iceland	Regulation & standards
17	Reykjavíkurborg	Iceland	Regulation & standards
18	Aranja ehf	Iceland	Technology aspects
19	EDIH Iceland	Iceland	Use cases
20	Ministry of Finance Iceland	Iceland	Use cases
21	no affiliation given	Iceland	Regulation & standards
22	no affiliation given	Iceland	Regulation & standards
23	no affiliation given	Iceland	Technology aspects
24	no affiliation given	Iceland	Use cases

Table 12 Participants of the Nordic countries' workshop

A.5 Documentation of the Italian workshop on March 14, 2023

Title of the workshop:

IDENTITÀ DIGITALE: QUALI PROSPETTIVE CON L'INTELLIGENZA ARTIFICIALE?

Title of the presentation of the IMPULSE-part of the workshop:

Intelligenza artificiale e blockchain nell' app IMPULSE e confronto con il sistema di identità digitale SPID (AI and blockchain in the smartphone IMPULSE app and a comparison with the current Italian eID SPID).

Who was in the workshop?

Hosts of the Italian workshop were Infocamere, Unioncamere and CyberethicsLab, our Italian project partners in IMPULSE. The Italian workshop was designed as a webinar with the main focus on the communication of the IMPULSE solution and discussion of implications in Italy. The webinar was organised in collaboration with the Digital Contact Point of the Genova Chamber of Commerce. The Digital Contact Point of the Genova Chamber of Commerce was created with the aim of spreading digital culture and tools to companies and enterprises and to support them in the adoption of new technologies.

In order to strengthen the impact of the webinar and add value to the IMPULSE project the webinar was shared with another EU co-funded project I-NEST in which Infocamere is a partner. I-NEST is one of the 13 Italian European Digital Innovation Hubs (EDIH) and was created in June 2022 by the European Union and the Ministry of Enterprise and Made in Italy to support the digital transition of small and medium-sized enterprises and public administration.

Concerning the organization, the organizers had produced a "save the date" poster as well as poster showing the agenda with speakers and title of the speeches. Both announcements were communicated about 10 days before the meeting on the web sites of the Chamber of Commerce and Unioncamere. The announcements were also used for social media communication. In detail Infocamere published 5 posts on Facebook, Linkedin, Twitter between 8th March and 14th March 2023 and Unioncamere published 29 posts on Facebook, Linkedin, Instagram, Twitter. All messages pointed to the project with general information, communication of the webinar, the Impulse video demonstrating how it works. Most of the links to social posts are reported on the common file social media on Teams sharepoint.

For the webinar, 81 persons had registered and finally there were 41 external experts participating in the event. Participants were mainly came from the private sector (companies) and the public sector (University, non-profit, public and local administrations).

The webinar took place on the 14th of March 2023. The organizers were located in Genova. Language of the webinar was Italian.

Agenda of the workshop

The 1h-online workshop had the following agenda:

- Introduction by the Genova Chamber of Commerce
- Presentation of I-NEST project
- Presentation of the IMPULSE solution, including pilots and technology aspects and a Q&A session
- Overview of eID-situation in Italy: Where we are now?
- Comparing the IMPULSE solution with the Italian SPID solution

For a more detailed agenda see the invitation poster in the annex. The slides used for the presentation can also be found in the annex.

Documentation of the workshop

Comparing the IMPULSE with the SPID-solution

One of the purposes of the workshop was to locate the IMPULSE solution within the national eID-landscape. As compared to the Italian solution SPID, the IMPULSE solution has the following characteristics:

- The registration (onboarding) process potentially eliminates human intervention to verify the individual's identity
- Data integrity is protected by the European EBSI infrastructure based on blockchain technology
- Simplified authentication does not involve passwords but only facial recognition
- Eventually IMPULSE will have the ability to manage multiple credentials related to the characteristics of a company or an individual (legal representative of a company, educational qualification, company certifications, certification of age of majority, etc.)

See slides in Annex B.

Use cases, challenges and concerns adopting digital ID systems in Italy

Questions asked were:

- Where can digital identity be used? (Public sector, private sector, etc.)
- What challenges/difficulties are involved in adopting digital identity in Italy?
- What are the main fears and concerns in adopting digital identity? (Privacy, data, etc.)

See slide number 14 of the Italian workshop in Annex B.

Documentation of the Q&A session

Some of the attendees noticed that IMPULSE could be well used in many domains and frameworks; the "citizen-Public Administration" dialogue is the first that comes up, even the "legal entity-Public Administration" dialogue looks quite appropriate to host IMPULSE, but even more "informal" framework looks fit for IMPULSE, for example the access to the gym, or to workplace, etc.

The current DI (SPID) is being adopted for the Public Authorities - citizen dialogue only.

Also access through a selfie is more attractive than using an user/psw, which makes IMPULSE more attractive and somehow handier than SPID.

The adoption of IMPULSE on a national level would not be such a big problem as Italian citizens are already used to SPID and to the use of the digital identity, on the other way a potential negative reaction could arise as citizens might feel forced to move away from a tool and land on a new one after "the effort they made" to learn and adapt to the previous one. Should the suggestion/imposition of adopting the new tool (IMPULSE) come from the public body, such a negative reaction is likely to appear.

Privacy, as expected, seems to be a very sensitive item. Questions such as "where are my data stored, can I keep them secured, who can check my personal data", etc. came from a number of attendees.

The possibility of using more types of credentials other than the "identity" has been discussed and it seemed very interesting.

The idea of having a sort of wallet (app) to store the identity credential and also the university credential, etc. is quite appealing. Someone in the audience is clearly referring to the eIDAS regulation and linking IMPULSE to the future eIDAS framework.

Finally some of the attendees asked about the difference between IMPULSE's identity and the certificates used to sign documents. The subject was discussed and explained to everyone.

Italy: Background report

In Italy, there are two eID systems in place that can be used to identify for e-government services: the electronic passport CIE with its CieID app for mobile use and the SPIS system:

The Carta d'Identità Elettronica (CIE) uses the information stored on the chip of the Italian passport. NFC capabilities are integrated since 2016. The identity provider is operated by the Ministry of the Interior. The electronic identity card allows Italian citizens to access e-government services through three authentication levels of increasing security: Access with a username and password (level 1), access with level 1 credentials and a one-time-password (level 2), and a smart card reader connected to a PC or an NFC-enabled smartphone to read the passport information stored on the chip.

To use the mobile authentication method, users need to install the CieID-app on their smart phones. The CieID app was developed by the Italian State Printing Works and Mint (Istituto Poligrafico e Zecca dello Stato) and is available for smartphones with Android 6.0 or above, or iOS 13 or above. Similar to the procedure used with German or French electronic passports, the Italian version requires a PIN (eight digits) for identification which, in Italy is put together by the number provided at the time of the request at the CIE issuance office and the number provided in the letter the issuance office sends with the ID. Once registered, citizens can identify themselves and unlock e-gov services by holding their passport close to their mobile and entering their PIN. To use the system, websites need to show the logo „Entra con CIE".

The CIE ID can be used for the following services:

- to identify for e-government services (and services of private entities?, unclear) as an alternative to the SPID system, or as
- tool for the digital signature (FEA, Firma Elettronica Avanzata) for which the app „CIE Sign" needs to be used.

The CIE can also be used to request a digital identity on the SPID system.

Sistema Pubblico di Identità Digitale (SPID) SPID is a federation, joined by several identity providers, but no banks. Identity providers have to be authorized by the Italian Agenzia per l´Italia Digitale.[8] Authentication is possible with a username and password, along with several variants of one-time-passwords, smart cards, or hardware security modules, leading to varying levels of assurance. Users are allowed to have several IDs, and none of them has to be necessarily government issued.

There are four different registration procedures to get an SPID ID:

- in person, at the offices of the digital identity providers or public administration counters that have activated a desk procedure.
- via webcam, with an operator made available by the identity provider or with an audio-video selfie, along with the payment of a symbolic sum by bank transfer;
- with CIE, the National Service Card and a smart card reader and a PC (requiring an PIN from the issuer of the CIE)
- with CIE and a smart phone using the apps of digital identity providers.[9]

Through SPID, citizens and enterprises were able to access online public services from over 5000 administrations in 2021. These include in the following domains: Agriculture, Environment, Energy, Justice, Education, Regional planning, Health, and Transport (European Commission; Deloitte 2021, p. 61f).

Since October 2021 a SPID ID is needed to access INPS (Tax, income and revenue service). It is planned to increasingly open public administration and government websites to the SPID system. In 2022, the number of

[8] Providers issuing SPID are: Aruba, Infocert, Intesa (Ibm Group), Lepida, PosteItaliane (PosteID), SielteID, Telecom Italia Trust Technologies, Namirial and Register.it. To get a SPID, users go to the website of one of these providers and register online for a SPID. After registering online, their app can be downloaded to the user´s smart phone.
[9] see www.spid.gov.it/en/what-is-spid/how-to-choose-between-digital-identity-providers/www.spid.gov.it/en/

Public administrations using SPID reaching 12,624. Private entities are also increasingly using SPID, with the number of entities growing to 151 in 2022 according to the Agenzia per l´Italia Digitale (2023).

Two popular initiatives have boosted the use of the SPID system: Italians who turned 18 in 2021 received a €500 bonus to spend on cinema, museums, concerts, cultural events, books. This measure is known as "Bonus Cultura." The same amount was granted to teachers for educational resources such as books, courses, and tickets to museums and theatres (Namirial 2022).

According to a press release of the Agenzia per l´Italia Digitale, more than 6 million SPID identities were issued during 2022, reaching 33.5 million as the total number of SPID identities (Agenzia per l´Italia Digitale 2023).

Banks, assurances, utilities and telcos in Italy have their own eID procedures. According to a survey by ID provider Namirial, Italian companies have started to integrate recognition methods without passwords or pins, replacing them with ownership factors, such as sending via SMS or email with one-time-passwords (42% of cases) or apps to generate one-time-passwords or push notifications (18%), but also biometric factors (only 8% of cases). The authors continue: „Even in more mature areas, however, there is a lack of an adequate internal structure that oversees the management of digital identity. And 63% of companies in these sectors have never evaluated the integration of nationally certified systems, such as SPID and CIE.“ (Namirial 2022)

Health: The Health Card („Tessera sanitaria“ - TS) enables access to health services provided by the Italian NHS - National Health System throughout the country. It is both an health insurance card and a tax code that allows citizens to receive medical treatments in EU countries. Although there are projects to digitize patients health records, telemedicine services, and online booking of appointments with doctors, there does not seem to be a connection with the eID systems in place yet.

Sources:

- Namirial (2022): State of play on adoption of Digital Identity in Italy 2022. Press release, December 1, www.namirial.com/en/news/digital-identity-state-of-play-italy-end-of-2022/
- Agenzia per l´Italia Digitale (2023): Italian Public Digital Identity System records over one billion logins in 2022. Press release of January 11, 2023, https://www.agid.gov.it/en/agenzia/stampa-e-comunicazione/notizie/2023/01/11/italian-public-digital-identity-system-records-over-one-billion-logins-2022
- European Commission; Deloitte (2021): Overview of Member States' eID strategies. CEF eID SMO Version 3.0, January 2021. Authors: Massimo Pedroli, George O'Neill, Arianna Fravolini et al.

Figure 12 Invitation poster for the Italian Workshop

List of participants

The following external experts participated in the Italian webinar:

Participant No.	Organisation
1	Camera Di Commercio
2	AMA GROUP
3	GIMISCO S.r.l.
4	Barbarini e Foglia Srl
5	asl
6	st Dellepiane
7	Scrittrice
8	IC Outsourcing
9	Smartpost Genova s.r.l.
10	BLU DIGITALPRESS
11	Mediaform scarl
12	B. & T. SOFTWARE & Service Snc
13	GIUSEPPE SANTORO Srl
14	Generazioni immobiliare
15	COLDIRETTI GENOVA
16	Teatro Stabile di Genova
18	GAFFURI CHIARA
19	private
20	Energia di FAETTI Tatiana
21	Crea Consiglio Regionale per L'economia agraria of Sanremo
22	Simul Tech
23	Srls
24	Cciaa Monte Rosa Laghi Alto Piemonte
25	Warrant Hub spa
26	Buda Maria
27	Oldrati Fabrizio
28	Paolo Cevasco
29	FOS SPA
30	Pittaluga
31	Camera di Commercio Genova
32	Gmg Net S.r.l.
33	Dintec Scrl
34	dintec
35	CCIAA GENOVa
36	Stoorm5
37	Università
37	ICO
38	Second Time Srl
39	ditta individuale
40	Aopd
41	Studio Legale Internazionale Justich

Table 13 Participants of the Italian workshop

A.6 Documentation of the German Workshop on March 30, 2023

Title of the workshop:

Smartphone-basierte digitale Identitäten mit Gesichtserkennung für öffentliche Dienste. Die IMPULSE-Lösung, Use Cases, Anforderungen.

Who was in the workshop?

Host of the German workshop was the Fraunhofer Institute for Systems and Innovation (ISI) research in Karlsruhe. Nicholas Martin and Bernd Beckert from Fraunhofer ISI have invited 54 experts via direct e-mail, of which 31 have registered for the workshop via the workshop website. Of these, finally 18 experts participated in the workshop. The experts were from banks, software firms, research institutes, ministries and local governments. Also, experts involved in the four implementation projects for secure eID systems of the German Federal Ministry for Economic Affairs and Climate Action (BMWK) called „Schaufenster sichere digitale digitale Identitäten“ were present.

From the IMPULSE-team, 11 persons were present at the workshop. The German workshop was the last in the series of the six dissemination workshops.

Agenda of the workshop

The 1,5h-online workshop had the following agenda:

- Presentation of the IMPULSE project including the pilots and technical aspects by Nicholas Martin from Fraunhofer ISI (15 min)
- Questions and answers concerning IMPULSE (5 min)
- Three break-out sessions discussing possibilities and barriers for the introduction of SSI-solutions like IMPULSE in Germany (use cases, technical aspects, regulation and politics) which started with an introductory round. The questions which were asked in the breakout sessions are shown at the beginning or the documentation of each session.
- Summary of the discussion and farewell (5 min.)

The slides used for the presentation by Nicholas Martin can be found in Annex B.

Documentation of the Q&A session

1. „Level of assurance“ of the IMPULSE solution

Q: A question concerning the „Level of assurance“ of the IMPULSE system. Self-registration via video in IMPULSE is significantly weaker than the videoident procedure. Therefore the question: For which applications is the IMPULSE system intended for?

A: The level of assurance in IMPULSE is "substantial". "High" cannot be achieved.

Q: Quite recently, there have been reports about how easily videoident systems can be circumvented. Since the IMPULSE-system is even weaker, have you made tests to show that the level „substantial“ can really be reached in IMPULSE?

Answer: We have not. But there is always still a manual check, so there is a person who checks the accuracy of the documents. That is how the level „substantial“ can be assured. In a next step in the project we will also do tests on the videoregistration.

2. The role of blockchain in the IMPULSE solution

Q: Is it true that when blockchain is used, personal data is fixed forever and cannot be changed?

A: The short answer is that in IMPULSE, no personal data is saved in the blockchain. Users' data is registered only on the smartphone. The only thing that is saved to the blockchain is the information about the service provider. So when the user accesses the website of the service provider, a check is done in the background that this is really the service provider and not not some other website.

Q: The principle of SSI is that in the blockchain the user's key is verified by the issuer. In the IMPULSE solution it seems that the issuer key is not in the blockchain but that only the relaying party is verified, i.e. the service provider with whom one wants to log in. Is that correct?

A: The question is basically about the role of blockchain in the system. Conventionally, in SSI solutions user information is often saved to the blockchain and the service provider checks the user information in the blockchain to verify the user. But in IMPULSE we turned this around so that no user information is saved to the blockchain but only the keys of the service providers. In fact, to store the user's information in the blockchain is kind of an outdated approach because it showed that this approach is not be compatible with the GDPR and the right of the user to forget information about themselves. So, most of the solutions started to remove this storage step. So now the information that used to be stored in the blockchain it not stored there anymore. But the issue remains to identify the person that presents a credential, which is the private key. It's owned by the user because it's linked with the centralized identifier of the user. That's the more recent approach and the approach we also use in IMPULSE.

Break-out Session „Use Cases“

In the session, four topics were discussed:

1. The state needs to invest, otherwise there are no use cases for eID solutions in Germany

2. But regulation requires secure eIDs, so there will be many use cases soon – even in Germany

3. If a secure eID comes with usability like in the IMPULSE solutions, then more people will use it

4. E-Government services are still missing in Germany

1. The state needs to invest, otherwise there are no use cases for eID solutions in Germany (or elsewhere)

Q: What added value can the IMPULSE solution or another SSI solution have?

A: I don't see any. The basic problem with all eID solutions is that no one is willing to pay money for them. That's why it's difficult to place such a product on the market. We have studied this in detail: Neither users nor service providers are willing to invest in such solutions. And where they are forced to invest in such solutions, for example in regulated areas such as online banking or e-government, where stronger authentication is required, that's where existing solutions such as Videoident are then used.

In our study, we asked users what they wanted, whether privacy was important to them, and whether they were willing to pay more money for more privacy, more money for secure identities, etc. - and the answer was always "no."

A: We held a citizens' workshop and a similar picture emerged: Willingness to pay for these services is rather limited, but in fact many people are of the opinion that digital identities are very important and that ensuring privacy is what matters here. And here, the big players like Google and Apple simply already seem to be further ahead.

A: Users are not willing to pay for eIDs because they get no benefit from providing a digital signature. In fact, the actual added value is at the verifier, he can then further process the process digitally and reduce transaction

costs. The signer has no direct added value, but should pay for it, that will not work. The users want to have a system that they can use and that meets certain requirements, but it should cost nothing. Because the other systems, which are not very secure, don't cost anything either. In principle, a significant benefit or added value is needed here, and probably very special solutions, to get people to switch from a free to a paid system.

It's a different story for companies or service providers, because they have added value, they have secure identities and digital processes. But it has to be said that it depends very much on the respective use case. Many of the use cases that are discussed again and again are in a trivial area where only a few Euros are at stake, such as the S-Bahn ticket. Here, you don't really need authentication at all, just payment. With the frequent things you need little security and with the rare things you need a lot of security. But these use cases are not so frequent, so no one is willing to pay for them in advance.

A: Our conclusion is that no one can operate the system if there is no money, and an ecosystem will not develop on its own. So if we want to replace the ID systems of Google, Facebook, etc., then the state has to make an advance payment, build something up, subsidize operators, etc., because no market will develop on its own.

2. But regulation requires secure eIDs, so there will be many use cases soon – even in Germany

A: In my opinion, there is also a market for eIDs in Germany and there are use cases. It is true that the value of identification is rarely with the user, it is with the provider of the service. But - and this is the reason why the use cases will develop: It is a regulatory requirement that we have this identification for many services, especially for e-government services.

Basically, we have two big problems with digitalisation in Germany: The first is that we have a relatively slow internet for such a developed country. And the second is that we don't have digital identities that work really well. This means that things that Germans often complain about in everyday life, such as re-registering when moving or registering a car, or any of the hundreds of use cases that we still have to deal with personally visiting offices, cannot be done digitally.

The regulatory system says that we have to have these identities, because it has to be ensured that I, as a user, am really the one who registers the flat or the one who talks to the doctor. That's why I see a very strong benefit for eIDs and it is the case that eIDs are increasingly demanded by the state. There are now laws that oblige companies to offer digital identities. So it's no longer a question of whether someone pays for it, but the state says you have to have it and that's why a gigantic market is developing here. In Germany, there are probably hundreds of companies working on this.

With regard to the added value of biometric SSI solutions, I see above all the future use of mobile phones, which enables very simple authentication and here the coupling with biometric solutions lends itself. SSI solutions generally offer a clear usability advantage.

The added value of eID solutions is simply that you have verified data. Because when users come with a sovereign identity, the service providers welcome that. Because they have an interest in the data that the user brings being checked and thus verified.

3. If a secure eID comes with usability like in the IMPULSE solutions, then many more people will use it

The IMPULSE solution as presented today will probably not be accepted by the German regulator, but in principle the approach is right. Because the added value that exactly this solution would offer is the simple user experience, i.e. you don't have to remember any passwords, then just take a quick look at your mobile phone or make a digital fingerprint and then you're in. In contrast, today's processes are very time-consuming. Especially the initial issuing process, which works via videoident and which is only possible during business hours. This process is error-prone and also very expensive. Simplifying this would be a very big step towards

increasing accessibility to digital services. Because the initial issuing process stops a lot of people from doing that.

But if you have the electronic identity on the mobile app, then you only have to log in for the service via biometrics, as we already know from the mobile phone. If this spreads, we will also be able to massively increase the number of cycles on the use cases. This will massively increase accessibility to the actual services. In terms of usability, I don't know of anything better than what they have presented with the IMPULSE solution.

The biometric procedure of the IMPULSE solution has the advantage that the credential cannot be used if the mobile phone is lost or stolen

Google and Apple rolled out passkeys on their smartphones last year and there, too, you can use biometrics to identify yourself without a password. And if the users of their smartphones are used to this for free in the next few years, then it will be more difficult to charge for it.

4. E-Government services are still missing in Germany

At the municipal level, the digital back-office area is still lacking in part, i.e. we are lagging behind here with the digital provision of public administrative services. That's why many administrative processes are require a signature at some point, which has to be provided locally. Nevertheless, I believe in a market for eIDs and believe that this will come.

In the city administration, end-to-end digitisation in the backend is a big topic right now and the administration will certainly be dealing with this for a few years.

It is also not yet clear how the federal account (BundID) can be linked to the different municipal accounts. We are currently still discussing this, it has not yet been clarified.

From an administrative point of view, the issue of costs for the eID is less relevant because they are not profit-oriented. But in the business sector with the B2B cases, there is possibly a higher willingness to pay again.

I see problems with the IMPULSE solution because I believe that the security level is not sufficient for Germany.

Break-out Session: „Technical aspects“

In the session, five topics were discussed:

1. Question about the achievable level of assurance of the IMPULSE solution

2. One single eID or many for different use cases with different levels of assurance?

3. Possible technical integration of the IMPULSE solution into existing German systems ELSTER and BundID

4. Could the face-ID of the mobile phone replace the selfie-ID procedure of IMPULSE?

5. What are the advantages of SSI solutions and what are their chances of implementation in Germany?

1. Question about the achievable level of assurance of the IMPULSE solution

Although we have been dealing with eIDs in the banking sector in Germany for some time, we were not yet aware of the IMPULSE solution. I was surprised by the approach. It is in the banks' interest to make facial recognition usable. But we need a high level of security, i.e. the level must correspond to „substantial“ or even

„high“. Because we banks are always committed to a high level of assurance for our use cases such as customer onboarding, strong customer authentication, etc.

For us, it is therefore crucial which security level can be achieved with IMPULSE. The credo and plea of the banks is that we would like to use the image data stored on the German eID to be used at least for verification. The image data would not have to be read out for this, but - if the Ausweisapp 2 would allow this - would be used to return a true or false after the image verification. That would be very interesting for us.

Before IMPULSE can be used in Germany, security aspects must be evaluated. And here the question is where the matching of the image material in the IMPULSE solution takes place from a technical point of view. In my opinion, this should be done in a "trusted execution environment". However, the developers are still far away from this; there is still no feasible way to realise something like this as standard across all smartphone models. In my opinion, the problem with the IMPULSE solution is that its tech stack does not allow a level of assurance beyond "normal" in Germany. The technologies currently used in the IMPULSE project do not even allow "essential", because image matching has to take place in the normal context of the app, where it has very little protection. The basic problem is: how do I make sure that someone else doesn't take a picture of me and use it to log in?

2. One single eID or many for different use cases with different levels of assurance?

And the question that arises in the context of eIDAS 2.0 and the Large Scale Pilots (LSP) that are now starting is how good it is to implement many different eID systems. Wouldn't it be better in the overall context of the EU to work together to create a uniform, EU-wide valid, interoperable and widely covering ecosystem?

In general, I have the impression that in Germany we are too concerned with the security level and not enough with usability. This focus limits the number of use cases and makes it more difficult to spread eIDs among the population. The lack of usability then again speaks in favour of having several systems on the market and trying out several approaches which then serve different use cases. But ultimately, the question for the end user is how many apps he or she is willing to feed with IDs in order to make use of them in the various use cases. And here I have to say, from a private end-user perspective, that I would really like to have a wallet, an app that allows me to handle both governmental, Europe-wide, interoperable use cases as well as normal economic use cases, such as online transactions via this app.

And the BundID, which can handle different levels of assurance, even the higher ones, has been designed for use of e-government services, and not for the private sector. The BundID is not yet open for normal private-sector use cases and it is unclear whether this will really happen in the future although there are different initiatives to do so.

The interpretation of the "Level of Assurance" is a bit different in Germany than in other countries in Europe. The BSI is somewhat stricter in its derivation of the eIDAS requirements into our national standards than eIDAS stipulates. So in general, the hurdle is higher in Germany than in other European countries. But this also means that we have to take this into account if we want to adopt solutions in Germany that have been developed elsewhere. These may not be acceptable in Germany. Also, if you look at the different eID solutions approved under eIDAS 1.0 in the different countries, the German solution with the digital ID card is one of the more secure solutions approved there for the "high" trust level.

This has both advantages and disadvantages. On the one hand, we have a very secure solution, but as is often the case with very secure solutions, the usability is not the best. We see this now with our identity cards (Ausweisapp 2), where many people criticise that the usability of the authentication medium is simply not as good as it could have been. Better usability is important and that is why there are many different eID projects. Better usability can greatly accelerate the spread of eIDs. Regarding the specific German interpretation of the security level, I think we should aim for standardisation in Europe in the context of eIDAS 2.0. That means we will have to try to achieve comparable security levels across Europe if we want to have a common ecosystem.

3. Possible technical integration of the IMPULSE solution into existing German systems ELSTER and BundID

In principle, we need diversity concerning wallets. One should not demand that every user has to install the same app, which then again comes from a central institution that then has too much power and control. On the other hand, it should be the case that all these apps are interoperable with each other. That is the real goal, to create a variety of solutions that can then communicate with each other. That is the big question with eIDAS 2.0, where we have a set of standards that is laid down in the reference framework. One could rely on this reference framework and say that all ID solutions shall implement the protocols and formats prescribed by eIDAS 2.0.

The question for the IMPULSE project would be which protocols and formats are used in IMPULSE and how interoperability with other solutions is addressed.

Our showcase project (Schaufensterprojekt) has agreed on a tech stack with the other showcase projects (IDUnion, etc.). It is important to know which technology the verifiers implement. If IMPULSE wants to dock there, it must be ensured that the credential from the IMPULSE app can be presented to the verifier. This means that you have to know which tech stack the verifiers implement. And if they all implement the same tech stack, they are compatible. I could now present the tech stack from our showcase project and then we could see whether IMPULSE can be docked here, yes, that would work.

If the goal is to implement IMPULSE in Germany, be it with ELSTER or with the BundID, then the question is always what protocols and standards it uses.

The question this raises for IMPULSE: Is the IMPULSE solution compatible with tech stacks specified in the ARF (European Digital Identity Architecture and Reference Framework) of eIDAS? Would it be possible for a verifier to set the W3C credentials directly to disclosure and so on? Here we would have to go deep into the technical details. The question is, would that be possible at this stage of the IMPULSE project?

4. Could the face-ID of the mobile phone replace the selfie-ID procedure of IMPULSE?

I wonder why you have to log in with your face every time in IMPULSE. In our project, users have an eWallet on their smartphone, comparable to the IMPULSE app. In order to use this app, users also have to authenticate themselves biometrically - with their fingerprint. If the phone doesn't allow fingerprinting, you have to enter the PIN pattern and as soon as the eWalltet is "unlocked", I can simply show my credential, verifiable by my private key-signed presentation.

It is unclear to me why it is necessary to film oneself in the IMPULSE solution. Because in our solution, you identify yourself with your fingerprint this unlocks the eWallet. This unlocking is coupled with the private key that is in the secure enclave, which means we can guarantee a high level of security.

With iPhones, the user unlocks the device via facial recognition. The question is why an additional activation via facial recognition is necessary in the IMPULSE system.

And I also see the selfie procedure in the IMPULSE project as critical in principle. This is because the recording often takes place in public spaces. And there can also be problems with the selfies in problematic physical conditions or even in bad weather or at night. My impression is that this is not necessary every time, it should be enough to simply look at the mobile phone. Pure image recognition is now inferior to iPhone face recognition.

5. What are the advantages of SSI solutions and what are their chances of implementation in Germany?

Q: Do we even need SSI solutions in Germany today and what are the advantages of SSI systems? Especially against the background of the introduction of the BundID, which means that this system is already available now that all citizens can use and that enables a high level of assurance (yet only for e-government services so far and not for business services)

A: A distinction must be made: BundID is an eID solution and SSI is a concept of how to implement eID solutions. Self-Sovereign Identity is a set of principles that explain how a digital identity can be deployed, used and stored under the full control of the user and owner of the digital identity. In my view, we will not get around SSI in Germany, because one solution proposed by eIDAS is an SSI Credential. The BundID will also become eIDAS-compatible.

For other SSI solutions this will mean that they have no place in Germany. At least not on the public side and possibly not for the private side either. Because then there will be the digital ID card and the BundID for all citizens and the issue of SSI in Germany will be, if not settled, then at least postponed far into the future.

However, these are special technical issues. For the average user, it is not clear what SSI is. The average user wants to be told that his data is safe and only he decides what happens with his data. What we as experts see as important aspects for acceptance, especially with regard to the security aspects, is often not so relevant for users.

Break-out session „regulation and standards“

In this session, three topics were discussed:

1. Regulation and standards can build trust in secure eID systems

2. eIDAS has to be implemented in Germany

3. The bank sector welcomes different solutions but not 27 for each country in Europe

1. Regulation and standards can build trust in secure eID systems

Security is an important aspect and if you can refer to certificates, regulations and the like, then you bring a "legal trust" into the system, which is very important. It is not enough to try to do this by technical means, trust must also be built up by standards.

Q: Will the qualified electronic signature be used in Germany in the future or do you still see obstacles here?

A: It depends on the security and the corresponding certifications. This means that certain standards must also exist concerning biometrics.

2. eIDAS has to be implemented in Germany

Q: From your point of view, what are the most important legal and regulatory requirements for implementing a digital identity solution like IMPULSE in Germany?

A: From my point of view, that would be eIDAS and - as soon as it has been passed - eIDAS 2.0. In addition, the technical guidelines of the BSI have to be taken into account and they are not always congruent with eIDAS.

We have strong guidelines from the EU, and we will also have to implement these nationally, e.g. within the framework of the Trust Services Act (Vertrauensdienstegesetz), which must be adapted to eIDAS. The question of how Verifiable Credentials could also be organised in the future as a trust service, i.e. as a system provider, will also play a role.

The corresponding standards and norms must be integrated into the implementing regulations in order to ensure that everyone adheres to the standards. Currently, there are still many question marks with regard to the

concrete design and implementation. Here, a harmonisation of eIDAS and future trust services must be achieved.

Ultimately, the IMPULSE solution raises the question of the "level of assurance". It is very important to check this and then also to be able to certify which level can be achieved.

3. The bank sector welcomes different solutions but not 27 for each country in Europe

From the bank's point of view, we have to identify people and there are different procedures. Here, systems are interesting for us in which legitimisation takes place immediately and without postal channels or other intermediate stages. But in the banking sector, there are other, stricter requirements as in other sectors, and here it would be exciting in principle to move in the direction of harmonisation.

Q: What do you expect from the European Commission when it comes to the spread of digital identity solutions?

A: The intention of eIDAS is right, it must go in the direction of standardisation and uniform solutions. And also interoperability, because there will certainly be different solutions. In Germany, we are curious to see how the eID infrastructure will work. Here we are interested in what comes out of the Large Scale Projects, to what extent the eID infrastructure and interoperability and cross-border cooperation really works. The financial industry has an interest that there are not 27 different national solutions in the end.

We hope that no further hurdles will be created, but that harmonisation will be promoted in general. And it is important that we have the appropriate regulatory foundations here that are necessary to bring confidence into the topic. However, care must be taken that these hurdles are not set so high so that there will be no more innovations. No market barriers or the like should be erected.

Background report: Germany

In 2023 there are two eID systems available for all citizens in Germany: The German eID and the BundID as a portal for **e-government services.**

The German eID is based on government-issued chip cards (eID cards) using certified chips and strong cryptographic protocols. Every German citizen owns a German eID because it is integrated in the German passport. With the renewal of the passport, citizens have received (via a postal letter) a PIN to activate the eID. The German eID can be used as a secure electronic identification for e-government services. It can be used from a PC using a card reader or with a mobile device using Bluetooth to read the information stored on the passport. The app needed to use the e-government services is called „Ausweisapp 2“. It currently allows to use about 50 services of public administrations (municipal, regional and national) in Germany.[10] In the "Smart eID" project, an eWallet solution for the German eID is being developed, in which the passport is digitally stored in the mobile phone. This currently only works with Samsung mobile phones because Apple does not release the Secure Enclave for third parties.

In mid 2023, there are about 6 million active users of the German eID system (citizens and business communicating with the public administration). The German eID can also be used for secure identification at the German tax office to submit tax refunds (www.elster.de) or to authenticate at the federal portal for e-government services called BundID (https://id.bund.de).

The BundID account is the user account of the federal state (Bund). Currently, the account can be used only for e-government services. The BundID system bundles the different municipal and regional e-government accounts and services. Gradually, all e-gov-services of the federal state as well as of the states shall be have moved to the BundID portal, so that there is a central Website for the majority of German e-gov services. Many

[10] A list of available services see www.ausweisapp.bund.de/anbieterliste

public services can be used today using the BundID, is planned to offer over 575 e-gov service categories on the platform. Citizens can identify themselves to the BundID portal in different ways: Via name and password (basic level), via name and the tax certificate Elster and password (substantial level) or via the German eID and password (high level). The BundID is eIDAS notified since 2020. In mid 2023, there are about 400.000 users of the BundID.

In addition to the efforts to establish a uniform e-government portal in Germany, the German Federal Government is supporting four projects in which alternative eID systems are being developed and implemented: ID-Ideal (an SSI-solution in Saxonia), IDunion (an SSI-solution in Cologne and Berlin), ONCE (a trusted services manager-solution for Hessen, Bavaria and North Rhine-Westphalia), and SDIKA (a combined central verifier and SSI solution for Karlsruhe and Heidelberg).

German banks have their own procedures with mobile TANs, which require postal letters or videoident procedures for customer onboarding. Banks are interested in eID systems but disagree on which systems to use.

Health sector: It is planned to have eIDs in the German health sector from 2024 onwards. Private and compulsory health insurance funds are each working on their own eIDs. In the future, the health eID is to enable the insured to use their smartphone instead of the insurance card to visit the doctor. In addition, the insured person can then use the digital identity to register for services such as the e-prescription app and the electronic patient file. A coupling with the German eID or the BundID is not planned.

Participant No.	Organisation	Interest
1	ING-DiBa AG	Regulation & standards
2	esatus AG	Regulation & standards
3	StMD	Regulation & standards
4	ING	Technology aspects
5	Ministerium für Wirtschaft, Innovation, Digitales und Energie des Saarlandes	Technology aspects
6	G+D Mobile Security	Technology aspects
7	Hochschule Mittweida	Technology aspects
8	Universität der Bundeswehr München	Technology aspects
9	AISEC FhG	Technology aspects
10	HTW Dresden	Use cases
11	Stadt Karlsruhe, IT Amt	Use cases
12	Landeshauptstadt Dresden Eigenbetrieb IT-Dienstleistungen	Use cases
13	ING Deutschland	Use cases
14	comuny gmbh (Mobiles Ausweisen. Softwarefirma Weinheim)	Use cases
15	HTW Dresden	Use cases
16	Fraunhofer IAO	Use cases
17	FZI Forschungszentrum Informatik	Use cases
18	Stadt Karlsruhe Amt für IT und Digitalisierung / Förderprojekt SDIKA	Use cases

Table 14 Participants of the Germanworkshop

Participants: External experts: 18, form IMPULSE-team: 11, total: 29

Break-out Sessions external experts: Use Cases: 9 , technical aspects: 6, regulation and standards: 3

Annex B Slides used in the workshops

Deliverable 6.2

Annex B: Slides used in the workshops

Impulse

Identity Management in PUbLic SErvices

Online Workshop

Smartphone-based digital identities using facial recognition for public services in Bulgaria

IMPULSE solution, use cases, adoption requirements

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

Impulse

Agenda

1. **Welcome**
2. **Overview IMPULSE: Project, Technology and Use Cases**
3. **Q & A**
4. **Discussion: Possibilities and Constraints for Adoption in Bulgaria**
   - Use Cases
   - Technology
   - Law and Regulation

Audio/Video recording:

We kindly ask for your permission to record the workshop
... but you may of course refuse!

Access to recordings will be strictly limited to IMPULSE team members

Recordings will be only used for research and documentation purposes

Recordings will be erased at the latest after project end in January 2024

Impulse

Agenda

1. **Welcome**
2. **Overview IMPULSE: Project, Technology and Use Cases**
3. **Q & A**
4. **Discussion: Possibilities and Constraints for Adoption in Bulgaria**
   - Use Cases
   - Technology
   - Law and Regulation

Impulse

Identity **M**anagement in **PU**blic **SE**rvices

General presentation of the project

Impulse

Who we are

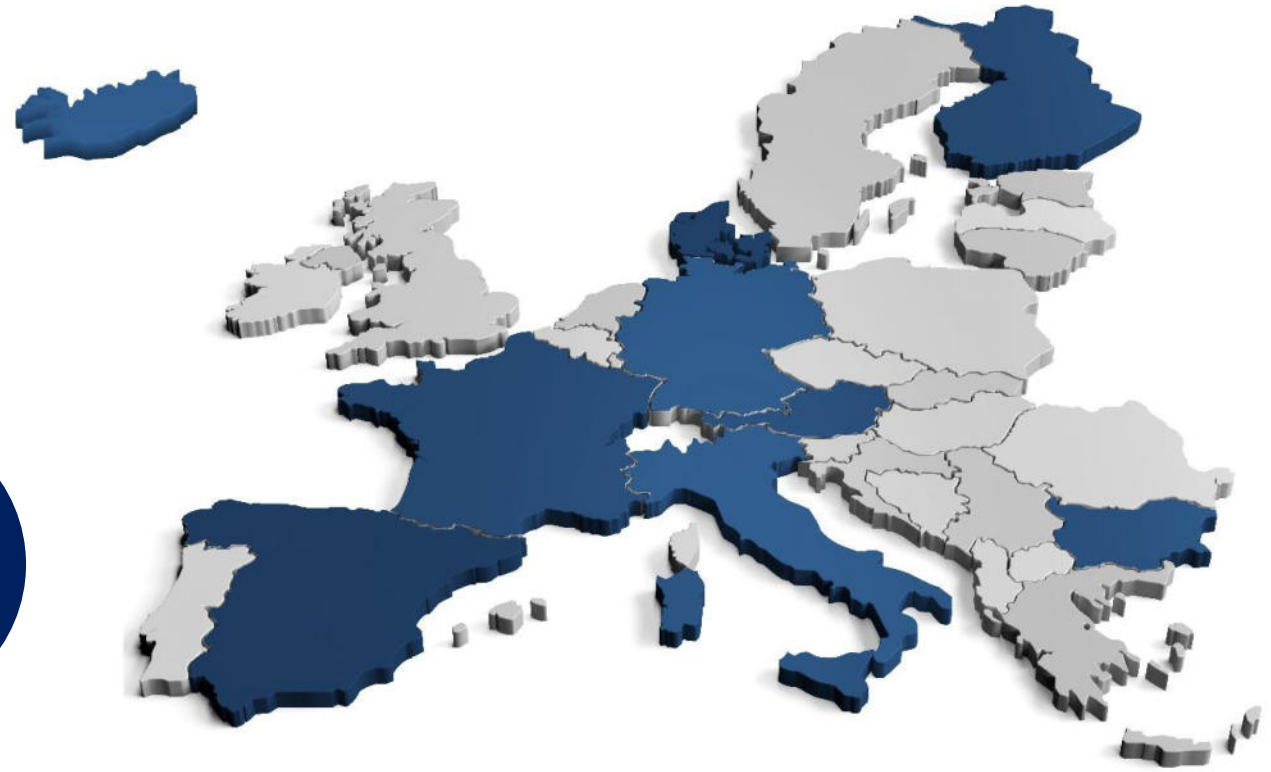
HORIZON 2020

LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

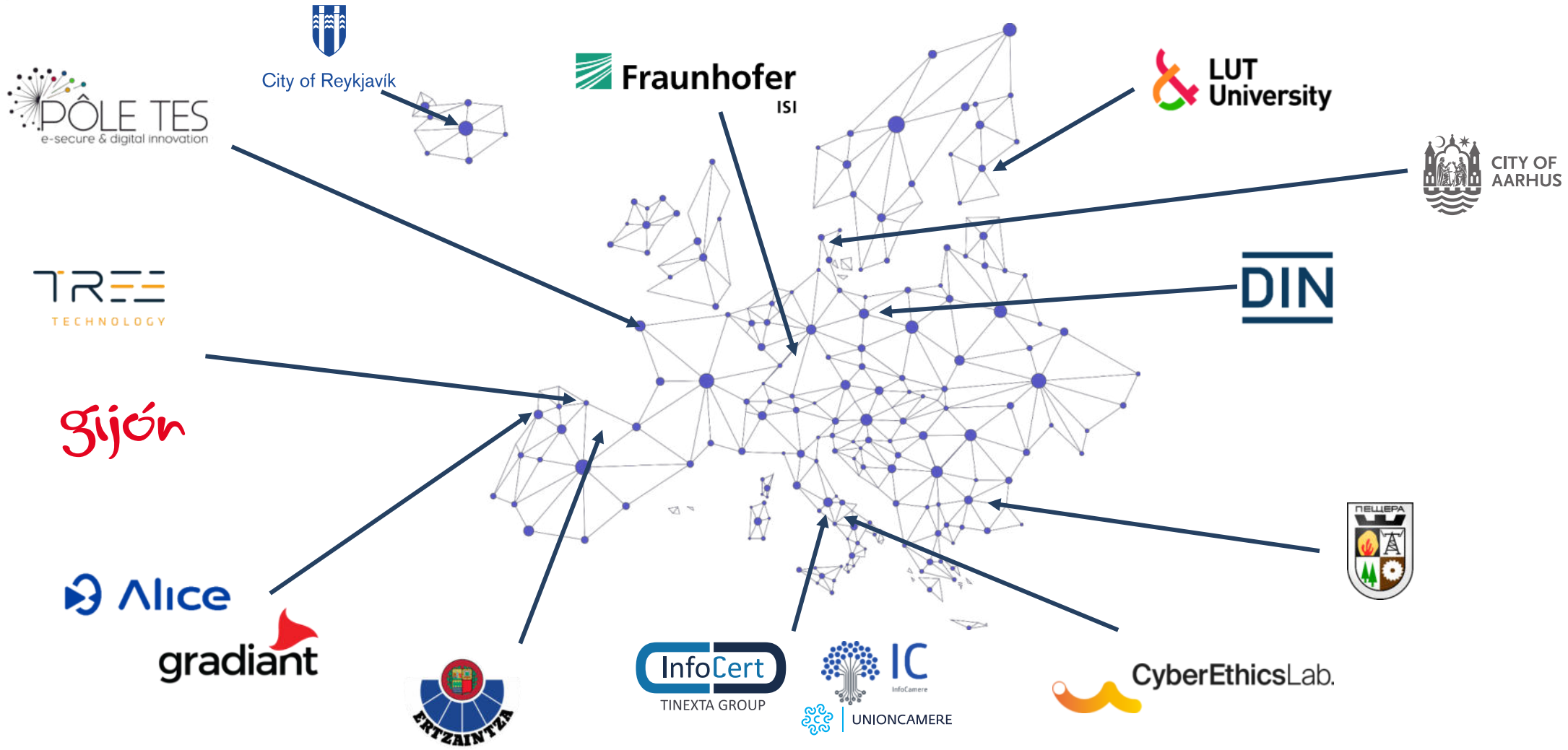
2021
2024

15 partners

+3M€



The consortium

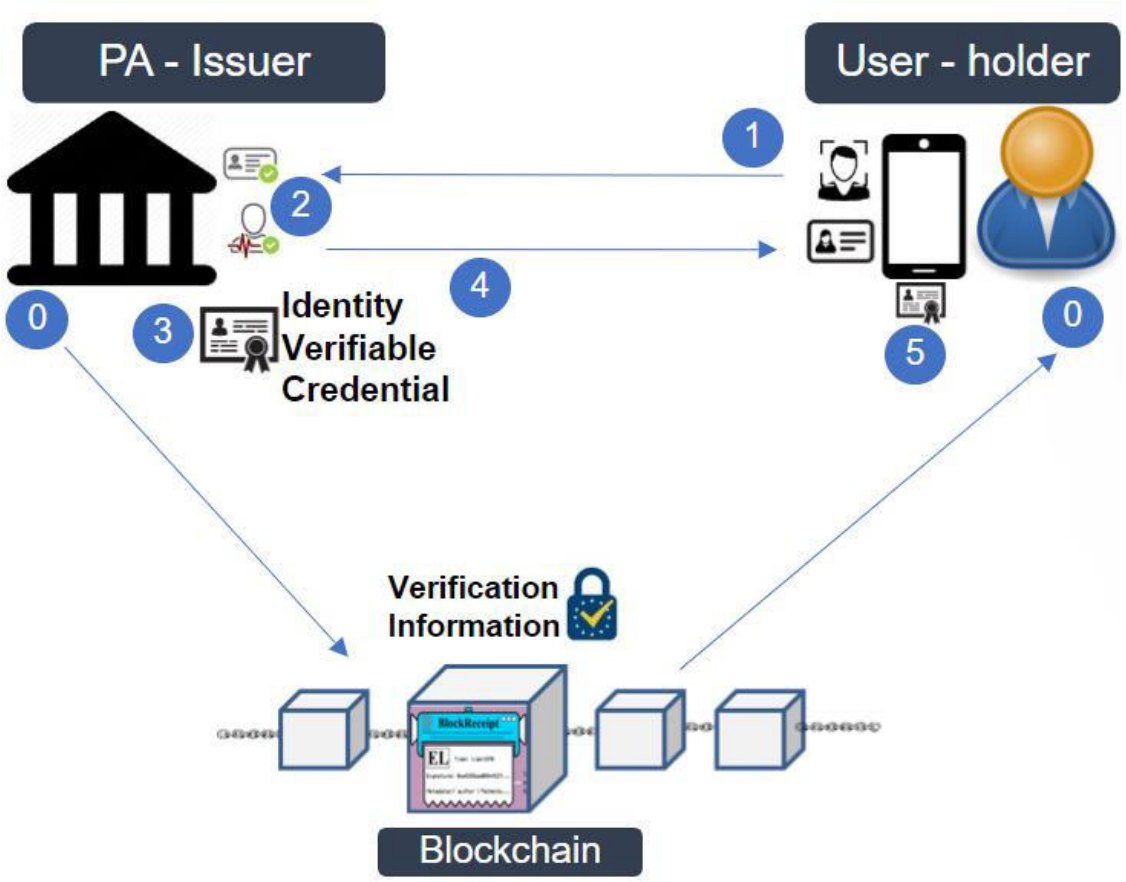


Impulse

Project Objectives

- Develop a decentralised, self-sovereign digital identity management system that uses facial recognition to authenticate the user
- Trial a basic version of the system in 6 public service use cases across Europe, including in Peshtera, Bulgaria
- Evaluate the socio-economic impact, develop frameworks for ethical and legal assessment, and support regulatory and standardisation efforts
- Further improve the system
- Develop roadmaps for possible future real-world deployments of the system

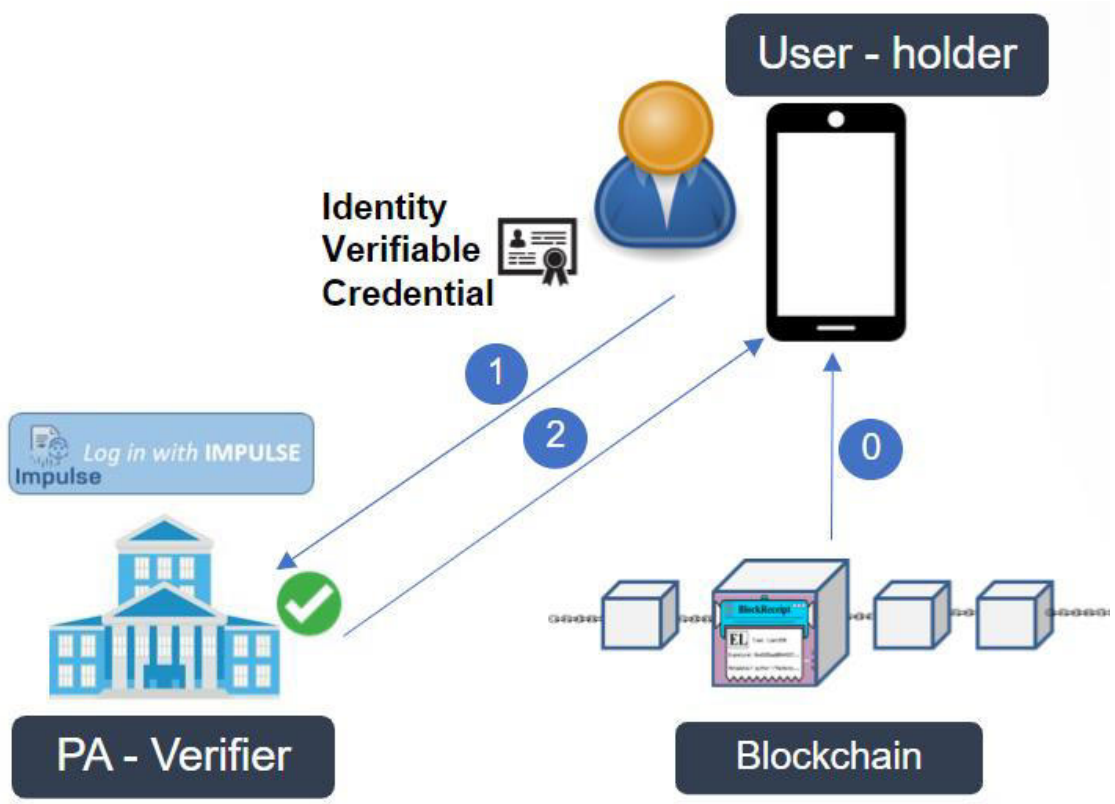
Overview of IMPULSE – User Registration



[0] Verification information (public keys) are stored on the Blockchain

1. User takes a selfie and a photo of their ID document (ID card, passport)
2. IMPULSE system uses AI to
   - check correlation btw selfie & ID photo
   - verify ID document
   - extract data from ID doc (name, etc)
3. IMPULSE system issues user with an Identity Verifiable Credential
4. Verifiable Credential is securely stored in the user's device
5. Verification information inscribed on blockchain

Overview of IMPULSE – User Authentication



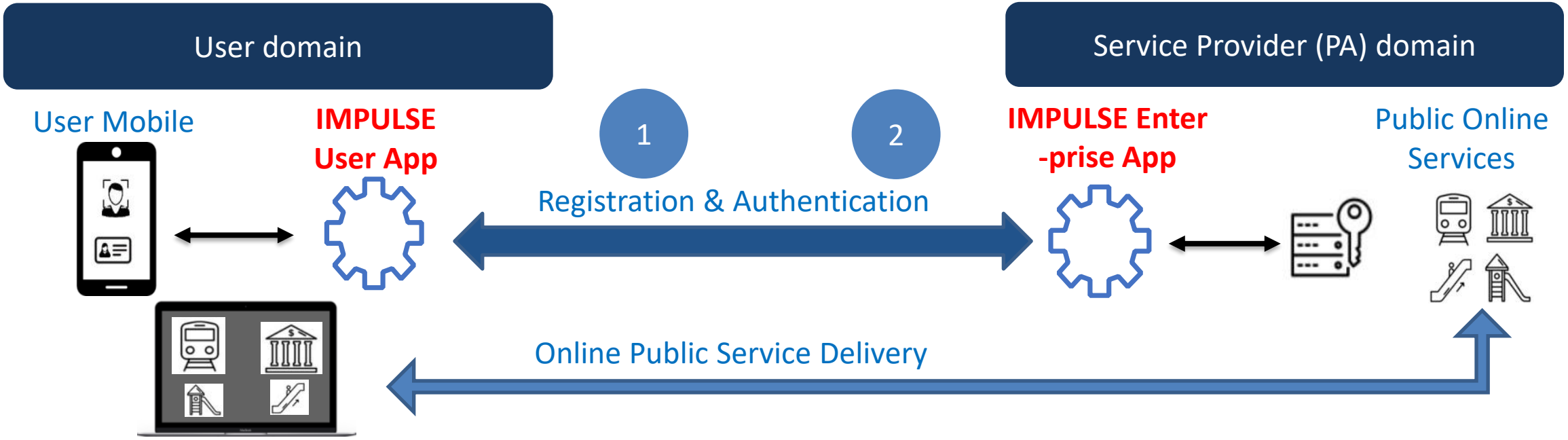
[0] User goes to PA website, chooses “Log in with IMPULSE”

[0] IMPULSE App opens and recovers verification information from the blockchain

1. User takes a selfie to authenticate to IMPULSE;
2. IMPULSE App presents the Verifiable Credential stored on the device to the PA
3. The PA confirms the Verifiable Credential and delivers the requested service to the User

Overview of IMPULSE – Integration & Instantiation

- Any online service can be integrated with the IMPULSE Digital Identity Management System
- → Install IMPULSE Android Apps (Google PlayStore), deploy a Container
- IMPULSE is based on EBSI/ESSIF ecosystem & EBSI Identity Verifiable Credential Schema



Overview of IMPULSE – Planned Improvements

- **Trusted Execution Environments:** for the Wallets in the User Application and the Enterprise Application
- **Remote QSeal Service:** Identity Credentials signed with a qualified signature
- **Informed Consent Service:** Management of the user consent by sharing data through Smart Contracts

IMPULSE Project: 6 Pilots

Impulse

City of Reykjavík

Reykjavik, Iceland
Better Reykjavik participatory democracy portal

Gijón, Spain
Public services app

Ertaintza, Spain
Issuing complaints entirely online

CITY OF AARHUS

Aarhus, Denmark
Electronic access to personal information and services

UNIONCAMERE

InfoCamere

Unioncamere & InfoCamere, Italy
Enterprise digital drawer

Peshtera, Bulgaria
Civil registration & certification

Impulse

IMPULSE in Peshtera, Bulgaria

Peshtera's Challenge: Low use of digital public services

Status Quo:

- A Digital Public Services Platform already exists (https://egov.bg) for >70 public services, but citizens hardly use it, preferring F2F service

Consequence:

- Civil servants spend much time on routine work serving citizens in person
- For citizens, getting public services takes a lot of time

Cause:

- Obtaining a digital identity is complicated & time-consuming
- Cost
- Low digital literacy

How can IMPULSE help?

- Simple Onboarding: getting a digital identity becomes much easier and faster
- Easy to use
- No additional software needs to be installed on your PC
- Saves civil servants time by simplifying and shortening the process of providing services to citizens

Pilot Activities in Peshtera

First "live" test of the IMPULE App with local citizens in October 2022

- Generally positive feedback...
  - Facial recognition for Log-In was fast & easy to use
  - Users liked that there were no passwords
  - Access to online services was fast
- ...But some improvements still necessary
  - Some confusion and need for help with the onboarding process
  - Notifications can still be improved
- Feedback now being analysed to further improve IMPULSE
- 2nd Iteration of the App expected in Spring 2023

Impulse

Agenda

1. **Welcome**
2. **Overview IMPULSE: Project, Technology and Use Cases**
3. **Q & A**
4. **Discussion: Possibilities and Constraints for Adoption in Bulgaria**
   - Use Cases
   - Technology
   - Law and Regulation

Impulse

Questions & Answers

Impulse

Agenda

1. **Welcome**
2. **Overview IMPULSE: Project, Technology and Use Cases**
3. **Q & A**
4. **Discussion: Possibilities and Constraints for Adoption in Bulgaria**
   - Use Cases
   - Technology
   - Law and Regulation

Impulse

Discussion

Possibilities and Constraints for Adoption in Bulgaria

Use Cases

In your view...

- **What are the main use cases for digital identity solutions in Bulgaria?**
- **What are the main requirements that digital identity solutions like IMPULSE must satisfy to be widely adopted?**
- **What are the main challenges to the adoption of new digital identity solutions like IMPULSE in Bulgaria?**

- **In Municipalities?**
- **In Central Government?**
- **In the Private Sector?**

Technology

In your view...

- **What technical requirements must digital identity solutions like IMPULSE meet to be adopted in Bulgaria?**
- **What are the key challenges to meeting these requirements? What technical concerns would you have about IMPULSE?**
- **What other eID systems exist in Bulgaria that IMPULSE must be interoperable with? What are the challenges here?**

- **In Municipalities?**
- **In Central Government?**
- **In the Private Sector?**

Law, Regulation and Policy

In your view...

- **What are the main legal and regulatory requirements that a digital identity solution like IMPULSE must meet in Bulgaria, including certifications?**
- **Which of these requirements tend to be hardest to meet?**
- **Can a biometrically-based digital identity like IMPULSE be used as a Qualified Electronic Signature?**
- **What can the European Commission do to support the diffusion of digital identity solutions in Bulgaria?**

Next Steps in the IMPULSE Project

- 2nd Iteration of the IMPULSE system and Piloting
- Complete impact assessment work
- Further workshops in other pilot countries
- Develop country-specific roadmaps

Identity Management in PUbLic SErvices

Thank you!

Georgi Simeonov simeonov@reap-bg.eu

Javier Gutiérrez Meana javier.gutierrez@treetk.com

Jaime Loureiro Acuna jloureiro@gradiant.org

Nicholas Martin nicholas.martin@isi.fraunhofer.de

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

Impulse

Identity Management in PUbLic SErvices

Taller Online

Soluciones de Identidad digital en servicios públicos y privados mediante el uso de registros distribuidos e IA

IMPULSE descripción, casos de uso, requerimientos.

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

Grabación de Audio/Vídeo:

Nos gustaría solicitar su permiso para grabar este taller con el fin de mejorar la solución IMPULSE
... Pero puede oponerse sin problema!

El acceso a las grabaciones estará estrictamente limitado a los miembros del equipo IMPULSE. Las grabaciones sólo se utilizarán con fines de investigación y documentación. Las grabaciones se borrarán a más tardar una vez finalizado el proyecto en enero de 2024.

Quiénes somos

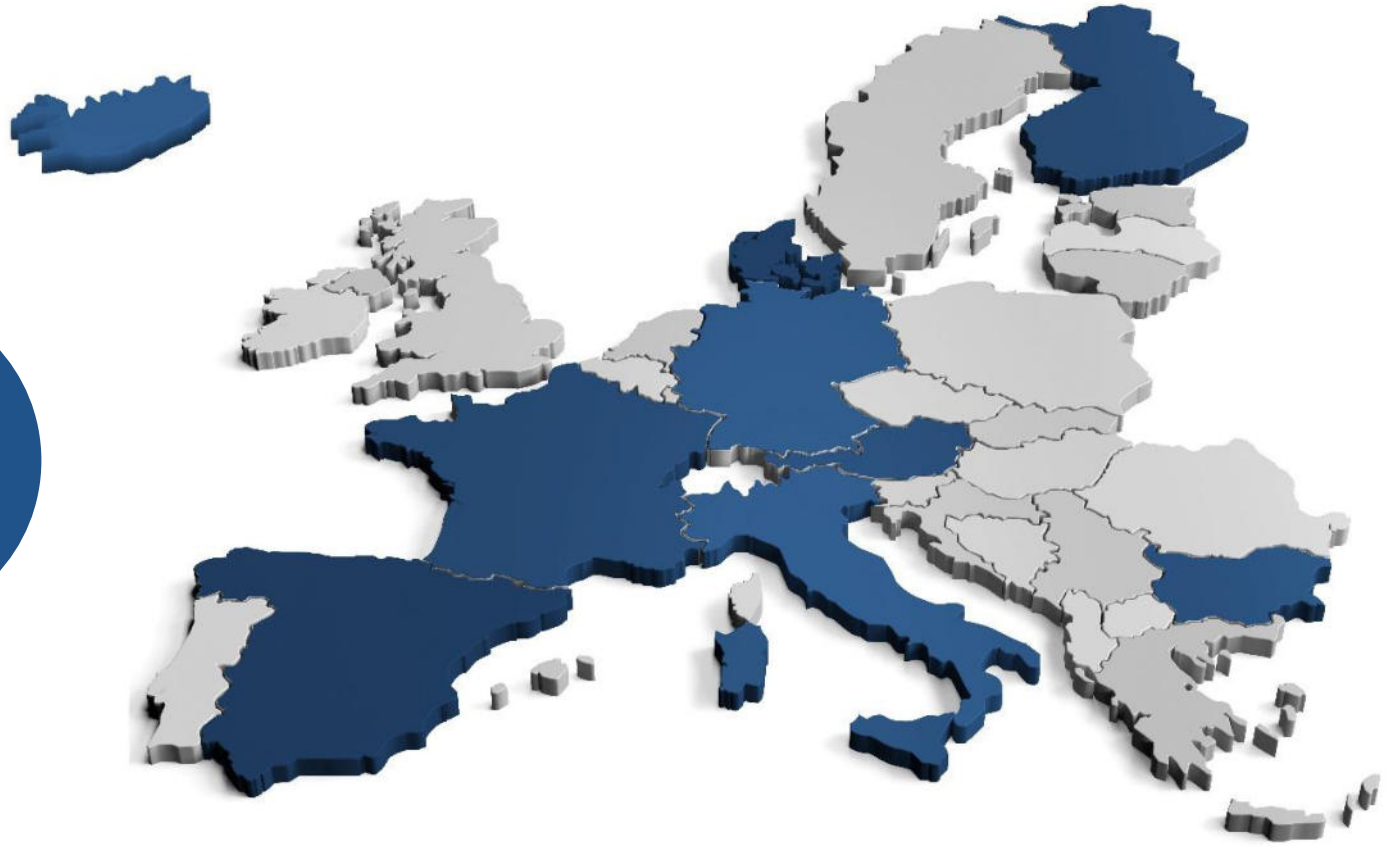
Impulse

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

2021
2024

15 Socios

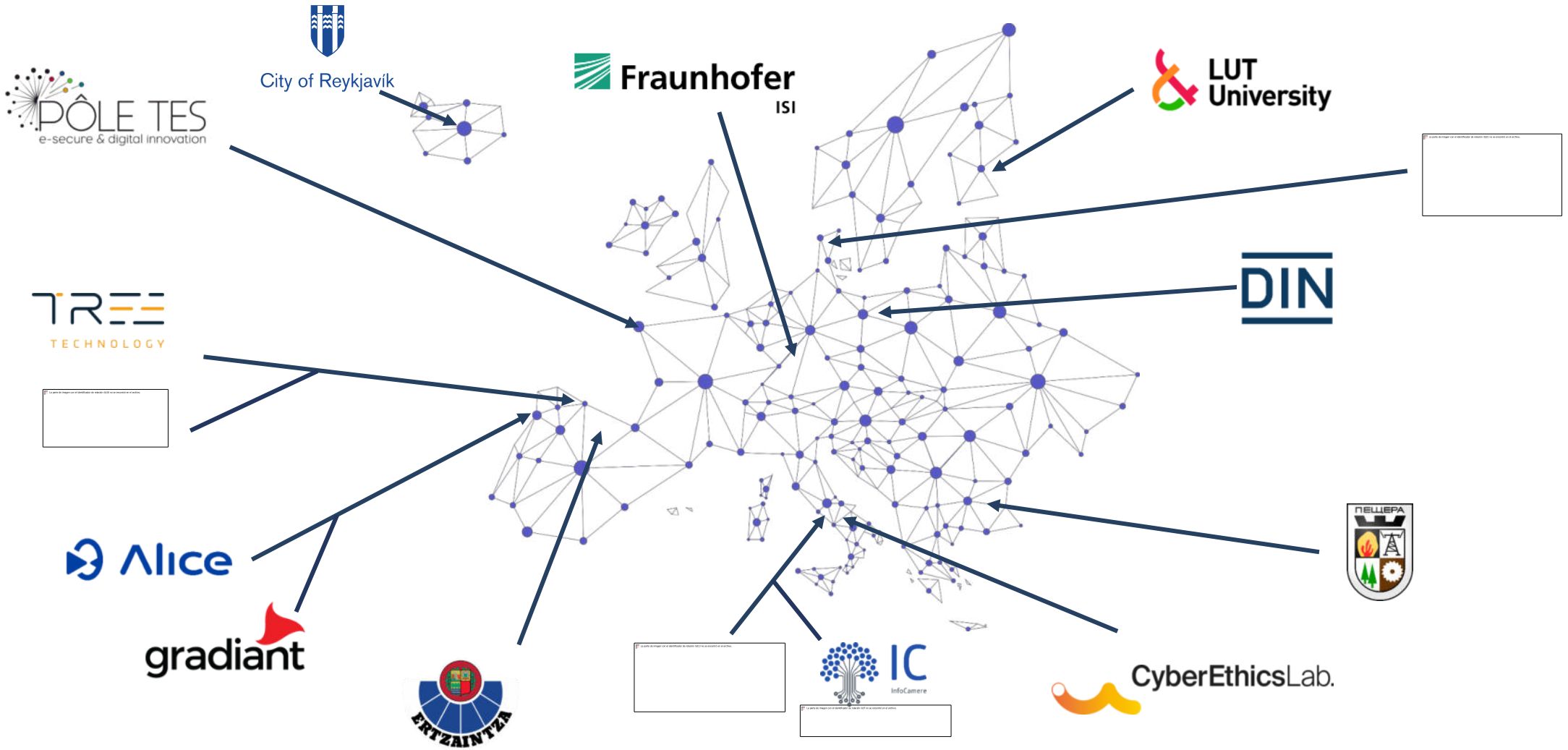
+ 3M €



[Transformative impact of disruptive technologies in public services]

Impulse

El consorcio



Objetivos del proyecto

- Desarrollar un sistema de gestión de identidad digital descentralizado y autosuficiente que utilice el reconocimiento facial como método de autenticación de usuario.
  - Logro al final del proyecto: Alcanzar un TRL 6 (**Sistema prototipo**).
  - Opciones tras la realización del proyecto: Desarrollar IMPULSE hasta un TRL 9 (comercialización) o reutilizar componentes individuales del sistema IMPULSE para nuevas soluciones. Ambas opciones conllevan la incorporación de nuevos socios.

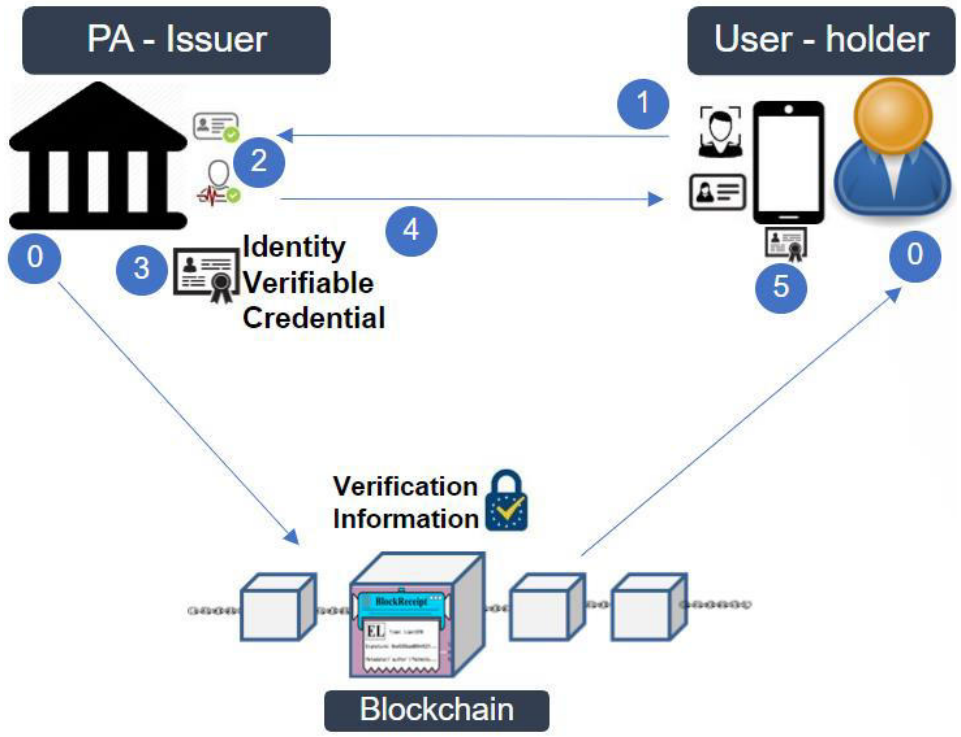
- Testar el sistema en 6 casos de usos en servicios públicos distribuidos por Europa.

- Evaluar el impacto, promover la reglamentación y la estandarización.

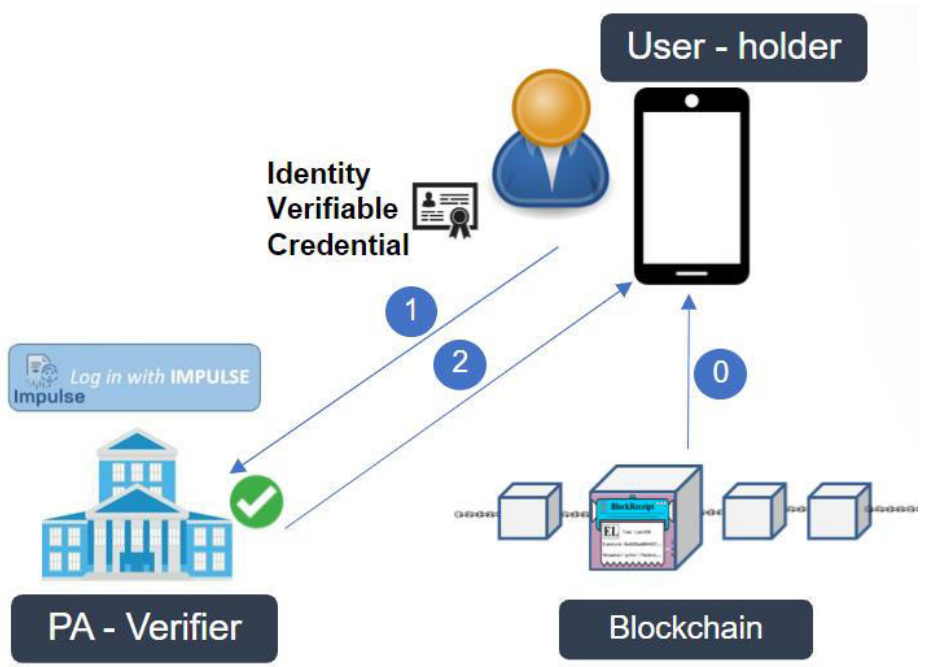
- Desarrollar hojas de ruta para posibles futuras implantaciones del sistema en el mundo real.

Visión general de IMPULSE

Registro / Alta de usuarios



Autenticación de usuarios



Impulse

DISCUSIÓN

Posibilidades y limitaciones para la adopción de IMPULSE en España.

Impulse

Sesión casos de uso

Casos de uso

Impulse

City of Reykjavík

Reykjavik, Iceland
Better Reykjavik portal democrático participativo.

Aarhus, Denmark
Acceso electrónico a información personal y servicios.

Gijón, Spain
Aplicación de Servicios Públicos

Unioncamere & InfoCamere, Italy
Plataforma digital para emprendedores.

Ertaintza, Spain
Quejas y denuncias online

Peshtera, Bulgaria
Registro y certificación civil

Casos de uso: Gijón

Estado del Arte

Desde hace más de 20 años Gijón apuesta por una Tarjeta Ciudadana que sirve para casi todos los servicios de indentificación y/o pago municipales. En la actualidad se han emitido más de 350.000 Tarjetas, siendo prácticamente universal dentro de Gijón

Hace 2 años lanzamos una nueva APP para acceder a varios de los servicios que se ofrecen mediante la Tarjeta Ciudadana. A fecha de hoy casi 60.000 personas han entrado a realizar algún trámite desde la APP

Necesidad de la Solución

El sistema de autentitación para acceder a la APP se basa en el Número de Tarjeta Ciudadana y un PIN de 4 dígitos. Sistema que existía hace 20 años cuando se lanzaron las primeras tarjetas. Y, aunque se toman medidas para mitiga los riesgos, es necesario buscar otras alternativas más seguras y sencillas para la ciudadanía.

Casos de uso: Gijón

Caso de Uso

Desarrollar un nuevo canal de acceso a la APP mediante la identificación de la persona con la solución de IMPULSE

Resultados de Pilotaje:

Actualmente algo más de 20 personas han realizado las pruebas. Por ahora podemos decir que en los resultados hay de todo, desde gente que ha realizado el proceso completo de forma autónoma sin problemas, hasta gente que no ha podido darse de alta con la nueva identificación por IMPULSE.

En esta fase y por motivos de seguridad las personas que se identifican mediante IMPULSE, solo pueden acceder a un servicio de consulta muy reducido y que no aporta información crítica.

Casos de uso: Ertzaintza

Estado del Arte

La Ertzaintza lleva apostando por la digitalización de los procesos de identificación desde hace años, con el fin de facilitar y hacer más sencilla la interacción de la ciudadanía con nuestra organización.

Necesidad de la Solución

Se necesitan soluciones que ya desde el inicio, el registro de los datos, sean ágiles, efectivas y seguras, garantizando la protección de los datos y los derechos fundamentales.

Caso de Uso

Pruebas de registro e interacción de personal del Departamento de Seguridad, garantizando la seguridad de los datos e informaciones registradas.

Casos de uso: Ertzaintza

Resultados de Pilotaje

Si bien inicialmente se contaba con unas 20-30 personas, los problemas de registro y funcionamiento de la aplicación ha llevado a realizar las pruebas iniciales con 5-7 personas, hasta se compruebe que la aplicación funciona correctamente, con el fin de garantizar procesos efectivos.

Además, se está comprobando las posibles incompatibilidades o dificultades que la aplicación puede presentar con la política de seguridad y las medidas implementadas derivadas de la misma.

Casos de Uso

Desde su punto de vista…

- **¿Cuáles son los principales casos de uso de soluciones de identidad digital en España?**
- **¿Cuáles son los principales requisitos que deben satisfacer las soluciones de identidad digital como IMPULSE para su adopción generalizada?**
- **¿Cuáles son los principales retos para la adopción de nuevas soluciones de identidad digital como IMPULSE en España?**

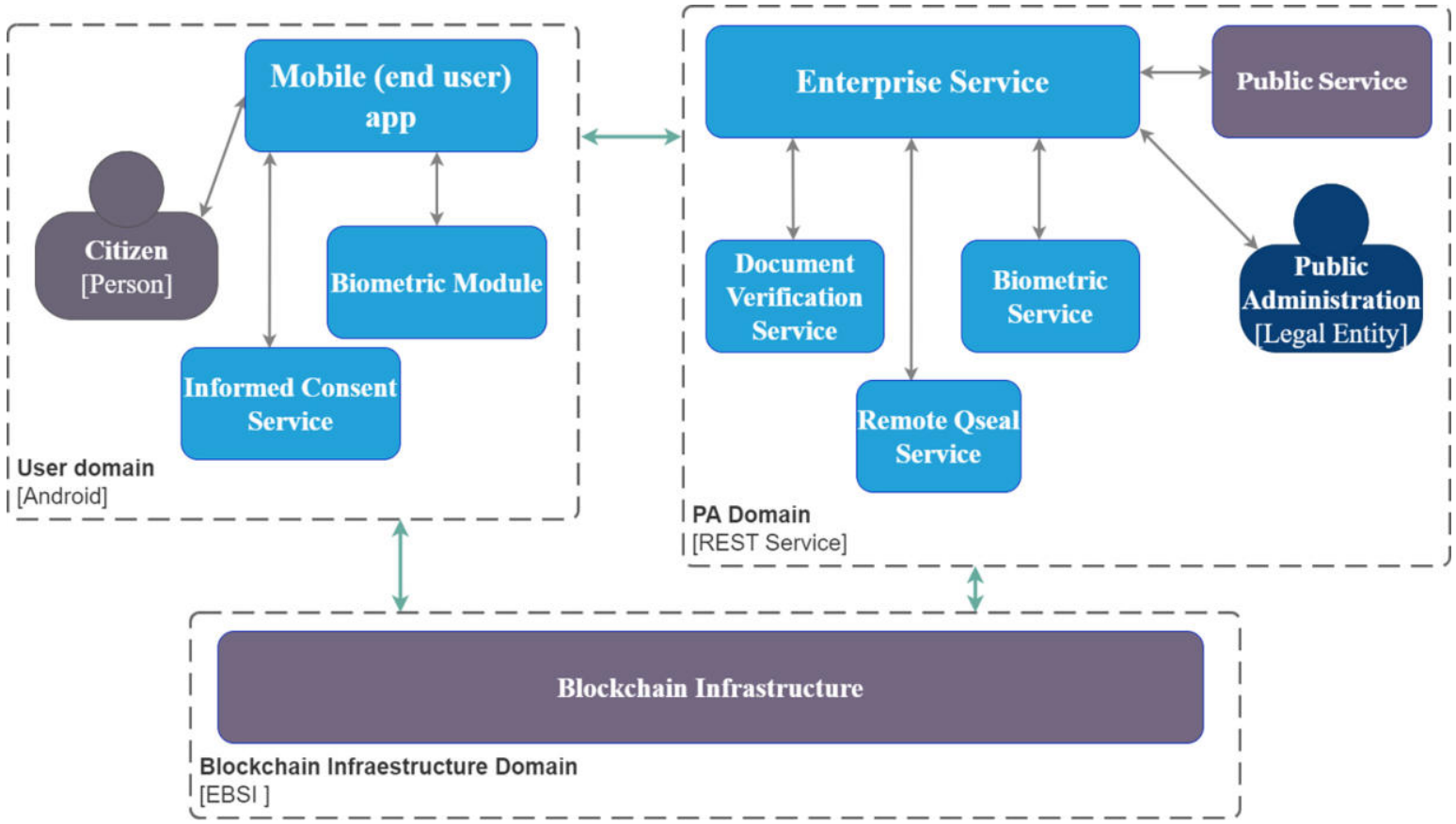
- **¿En Ayuntamientos?**
- **¿En Gobiernos Centrales?**
- **¿En el Sector Privado?**

Impulse

Sesión técnico- legal

Impulse

Tecnología



VIDEO

Sesión Técnico - legal

Impulse

Desde su punto de vista…

- **¿Qué requisitos y retos técnicos deben cumplir las soluciones de identidad digital como IMPULSE para ser adoptadas en España? ¿Qué preocupaciones técnicas le suscita IMPULSE?**
- **¿Qué otros sistemas de identificación electrónica existen en España con los que IMPULSE debe ser interoperable? ¿Cuáles son los retos?**
- **¿Cuáles son los principales requisitos legales y reglamentarios que debe cumplir en España una solución de identidad digital como IMPULSE, incluidas las certificaciones?**
- **¿Qué puede hacer la Comisión Europea para apoyar soluciones de identidad digital como la de IMPULSE en España?**

Visión General de IMPULSE – Mejoras Programadas

- **2ª** Iteración del sistema IMPULSE y **Pilotaje**.
- Completar el trabajo de **evaluación de impacto**.
- **Nuevos talleres** en otros países piloto.
- Elaboración de **hojas de ruta específicas** para cada país.

Impulse

Identity Management in PUbLic SErvices

Iria Núñez inunez@alicebiometrics.com

Javier Gutiérrez Meana javier.gutierrez@treetk.com

Iñaki Gangoiti Torrontegui igangoiti@seg.euskadi.eus

Luca Mattei l.mattei@cyberethicslab.com

Tetiana Vasylieva t.vasylieva@cyberethicslab.com

Pedro López Sánchez plopez@gijon.es

Xavier Martínez xmartinez@gradiant.org

Jaime Loureiro Acuna jloureiro@gradiant.org

Muchas Gracias!

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

Impulse

Identity Management in PUblic SErvices

Identité numérique et services publics

Quels technologies, moyens, impacts et future exploitation ?

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

PROGRAMME

Présentation générale

10:00 Présentation de la solution IMPULSE

10:20 Session Questions/Réponses

Sessions de discussion participatives

Session 1
10:30
11:00

Room 1 : Aspects technologiques – Facilitatrice : Bertille AUVRAY
Blockchain, IA, biométrie, reconnaissance faciale pour une identification numérique sûre et autonome

Room 2 : Études de cas – Facilitatrice : Marie PEREDA
Méthodologie, besoins des utilisateurs, attentes des secteurs publics et privés

Session 2
11:00
11:30

Room 3 : Impact du développement des solutions eID – Facilitateur : Benjamin CHERET
Réglementations, normes, éthique, législation et droit

Wrap-up

11:30 Restitution des premiers résultats et tendances & Sessions Questions/Réponses

12:00 Fin de l'atelier

Impulse

Impulse

Identity Management in PUblic SErvices

Présentation générale du projet

Impulse

Le **projet**

HORIZON 2020

LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

2021
2024

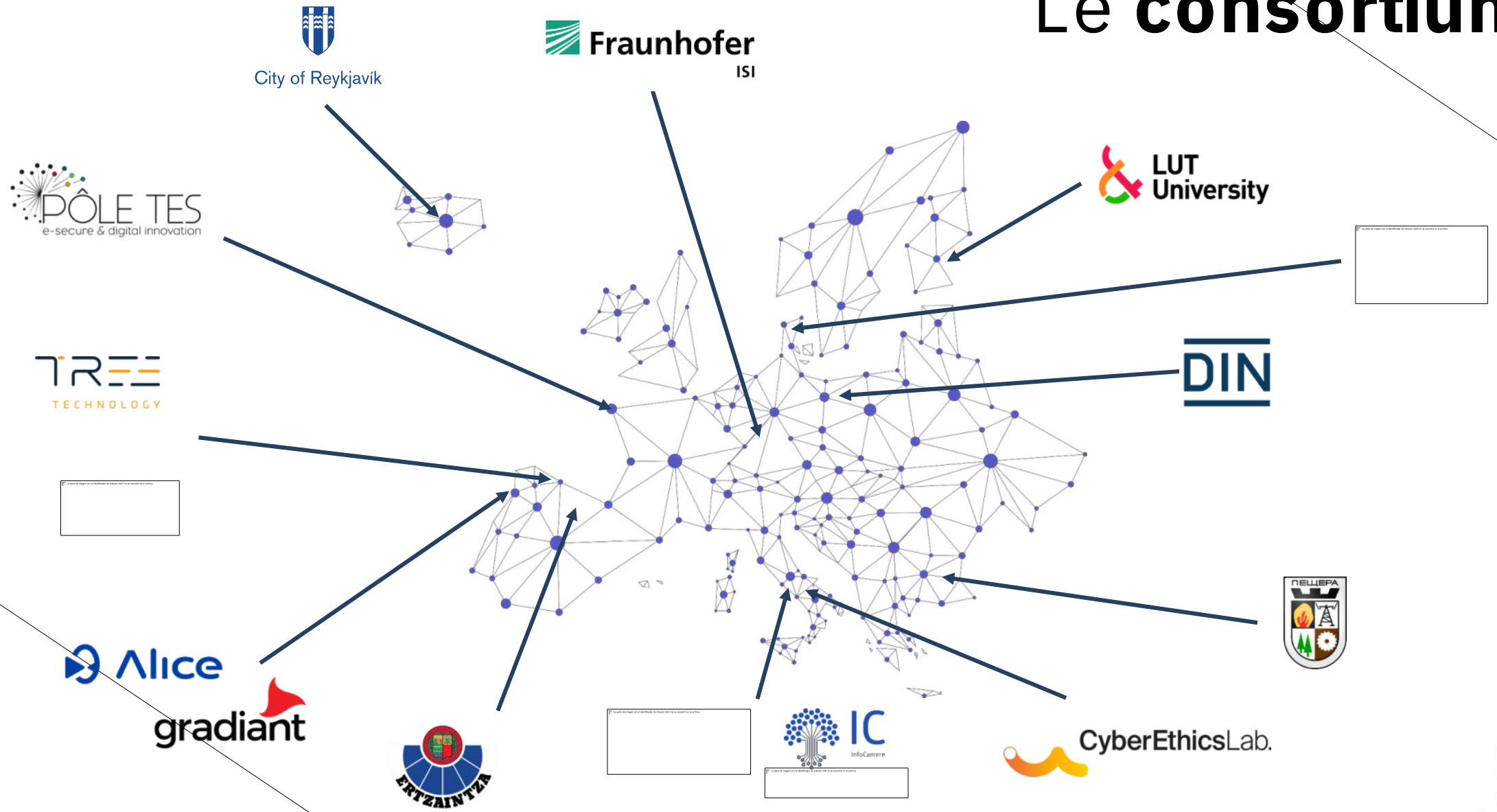
15
partenaires

+3M€

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

Impulse

Le **consortium**



Impulse

Les **objectifs**

IMPULSE vise à développer
une **méthode d'évaluation** de la gestion de **l'identité électronique**
(identification individuelle)
lors de l'utilisation des **services publics en ligne**,
grâce à l'utilisation de l'**intelligence artificielle** et de la **blockchain**.

Evaluation

- **Avantages**
- **Risques**
- **Coûts**
- **Limites**

Impacts

- **Socio-économiques**
- **Juridiques**
- **Ethiques**
- **Opérationnels**

Conditions cadres

- **RGPD**
- **Règlements eIDAS**
- **Systèmes et normes nationaux existants**

Impulse

Résultats **attendus**

Cadre pour une intégration de l'IA et de la technologie blockchain en matière d'eID

Des **feuilles de route pour le déploiement, l'adoption et la pérennisation des technologies d'identification électronique par les services publics**

Impulse

Les **technologies**

OPPORTUNITE DE L'UTILISATION DES TECHNOLOGIES DISRUPTIVES

Intelligence Artificielle

Authentification biométrique

Vérification de documents

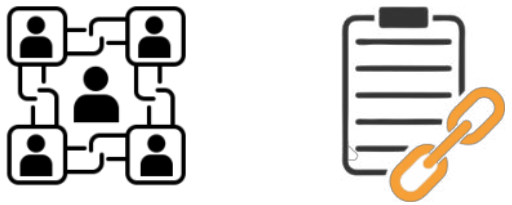
Enregistrement numérique

Blockchain

Registre distribué (DLT)

Contrôle de l'utilisateur sur ses données

Smart contracts



Impulse

Cas **pilotes**

City of Reykjavík

Reykjavik, Iceland
Portail de participation démocratique *Better Reykjavik*

Aarhus, Denmark
Accès électronique aux informations et services personnels

Gijón, Spain
Public services app

Unioncamere & InfoCamere, Italy
Dossier numérique des entreprises

Ertaintza, Spain
Dépôt de plainte en ligne

Peshtera, Bulgaria
Enregistrement et certification de l'état civil

Impulse

1ere itération des **cas pilotes**

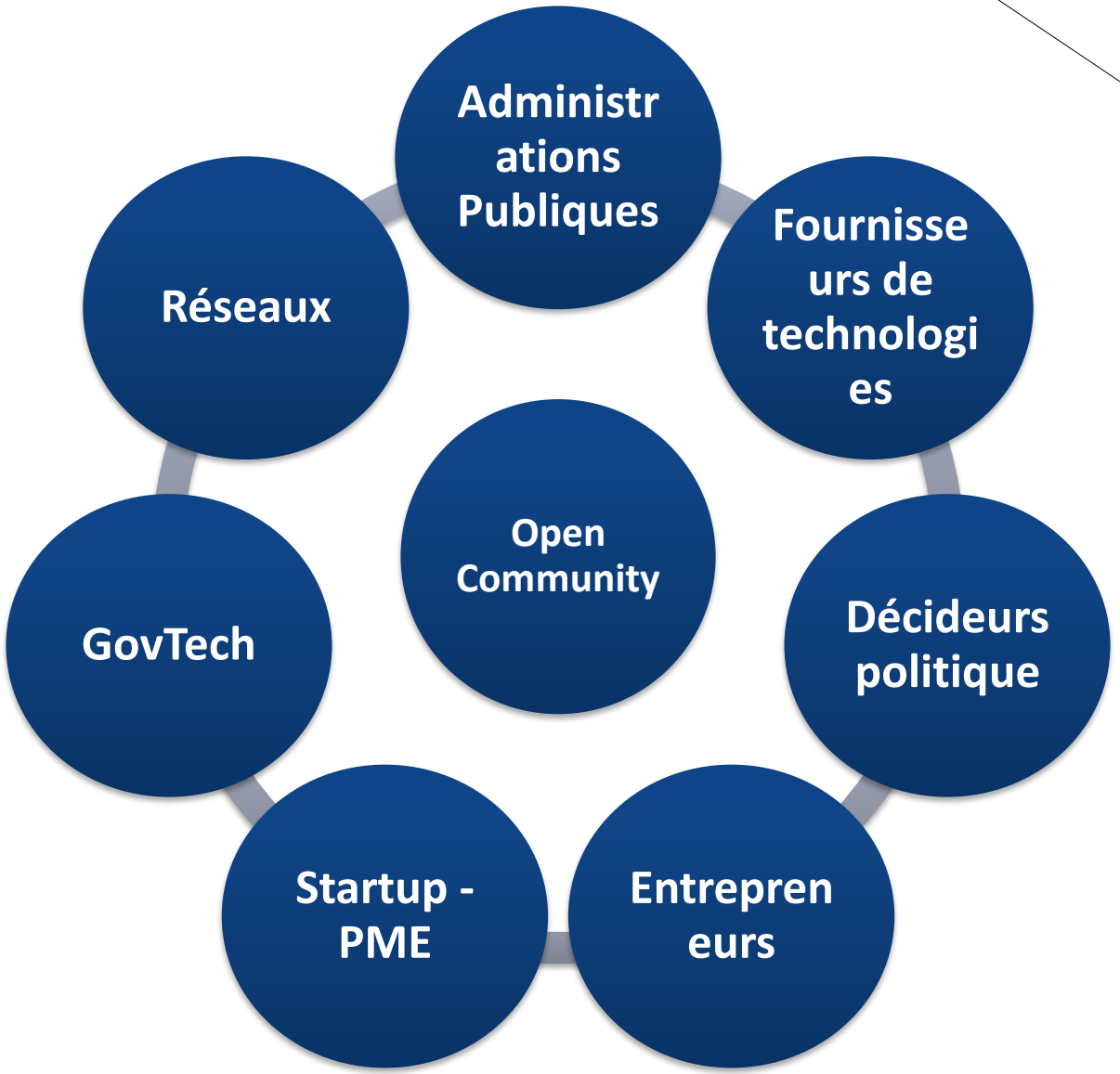
- **Défis techniques lors de la mise en place de la solution IMPULSE sur les sites de cas**
- **L'onboarding a été un peu lourd**
- **Manque d'informations si quelque chose fonctionne ou échoue**
- **Pas de politique de confidentialité ou d'information sur le stockage des données**
- **Certaines parties de l'application étaient confuses**
- **Que se passe-t-il si les caméras ne fonctionnent pas correctement ou ne sont pas assez bonnes (mauvaise qualité d'image) ?**

- **La majorité a perçu la reconnaissance faciale comme sûre et digne de confiance, ainsi que plus facile et plus sûre que les autres identifications biométriques.**
- **L'identification est rapide et la solution est facile à utiliser.**
- **La solution constitue une bonne (ou meilleure) alternative aux systèmes actuellement en place et la plupart l'utiliseraient à l'avenir après des améliorations techniques.**
- **Dans l'ensemble, la solution est considérée comme sûre (avec quelques réserves).**

Impulse

Volonté de **collaborer**

Pour obtenir des effets significatifs, faire accepter et promouvoir l'adoption de concepts d'identification électronique perturbateurs dans les services publics, la collaboration avec les parties prenantes externes est cruciale.



Impulse

Comment une seule solution d'identification électronique adaptative peut être utile à tout un écosystème,

des citoyens au gouvernement ?

Impulse

Impulse

Identity Management in PUblic SErvices

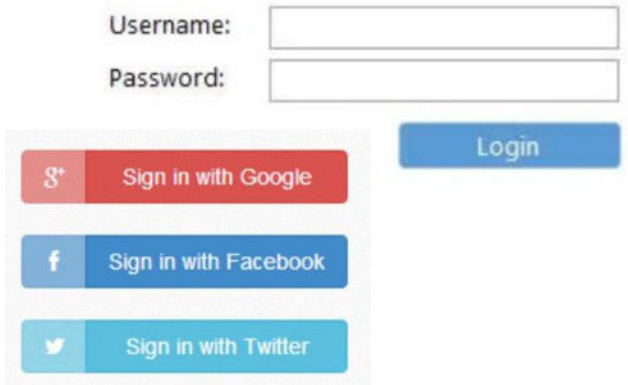
Aspects technologiques
Blockchain, IA, biométrie, reconnaissance faciale pour une identification sûre et autonome

Facilitatrice : Bertille AUVRAY

Impulse

IMPULSE comme **alternative décentralisée**

Les systèmes traditionnels et existants de gestion des identités électroniques sont basés sur des architectures centralisées qui sont contrôlées par des tiers (potentielles fuites des données et ou un non respect de la vie privée des utilisateurs), de plus les utilisateurs utilisent généralement un mot de passe faible ou identique sur de nombreux sites, etc.



IMPULSE vise à mettre en place un système de gestion des identités électroniques **décentralisé** et **auto-souverain**, basé sur un modèle d'**identifiant vérifiable** (Verifiable Credential – VC) sur la blockchain. Non seulement les problèmes techniques, mais aussi les problèmes d'inclusion et d'expérience d'utilisation.

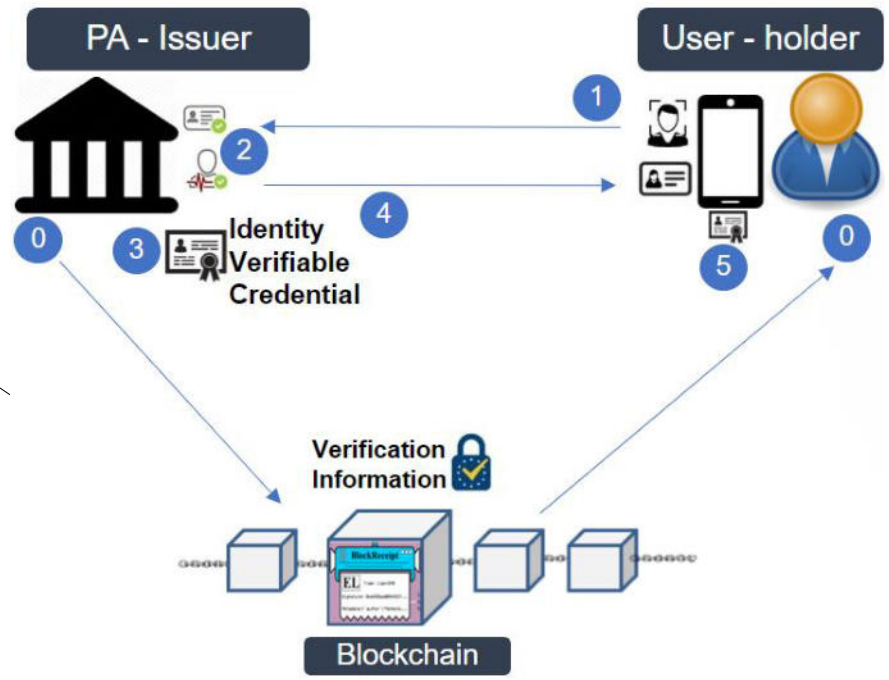
- **Décentralisé** : Il n'y a pas d'entité centralisée en charge de l'identité de l'utilisateur.
- **Identité auto-souveraine** (Self-Sovereign Identity – SSI) : Les données d'identité de l'utilisateur restent sous son contrôle
- **Modèle VC** : Un VC est un ensemble de déclarations cryptographiques non répudiables qui contient les attributs d'identité de l'utilisateur (par exemple, le nom, le nom de famille, le code fiscal, le numéro de compte de paiement, etc.)

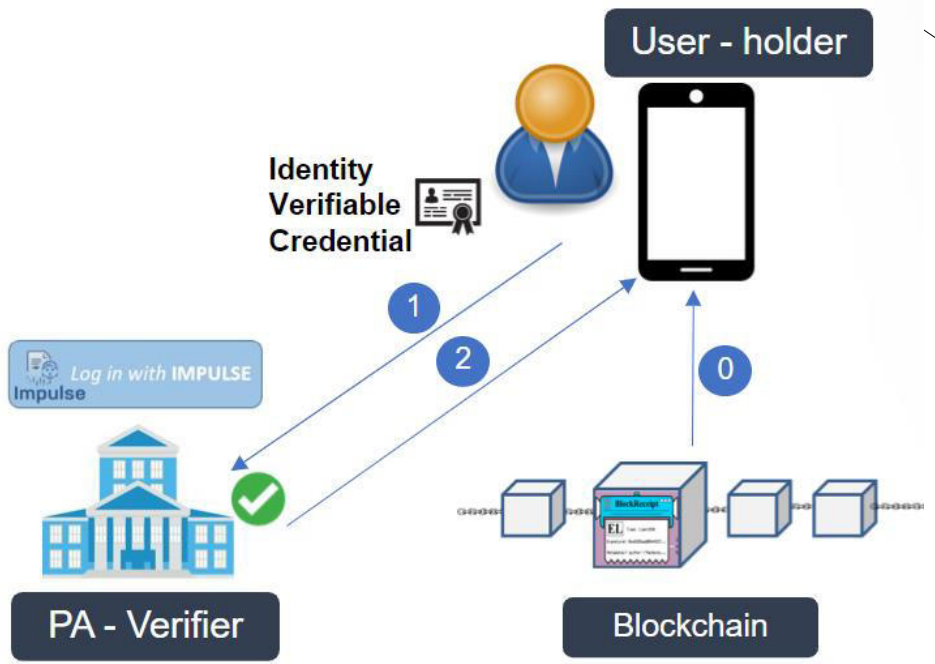
Impulse

IMPULSE comme alternative **décentralisée**

Processus d'enregistrement des utilisateurs

Un utilisateur demande sa carte d'identité vérifiable par le biais d'un processus d'embarquement numérique basé sur la reconnaissance faciale et la validation de documents.



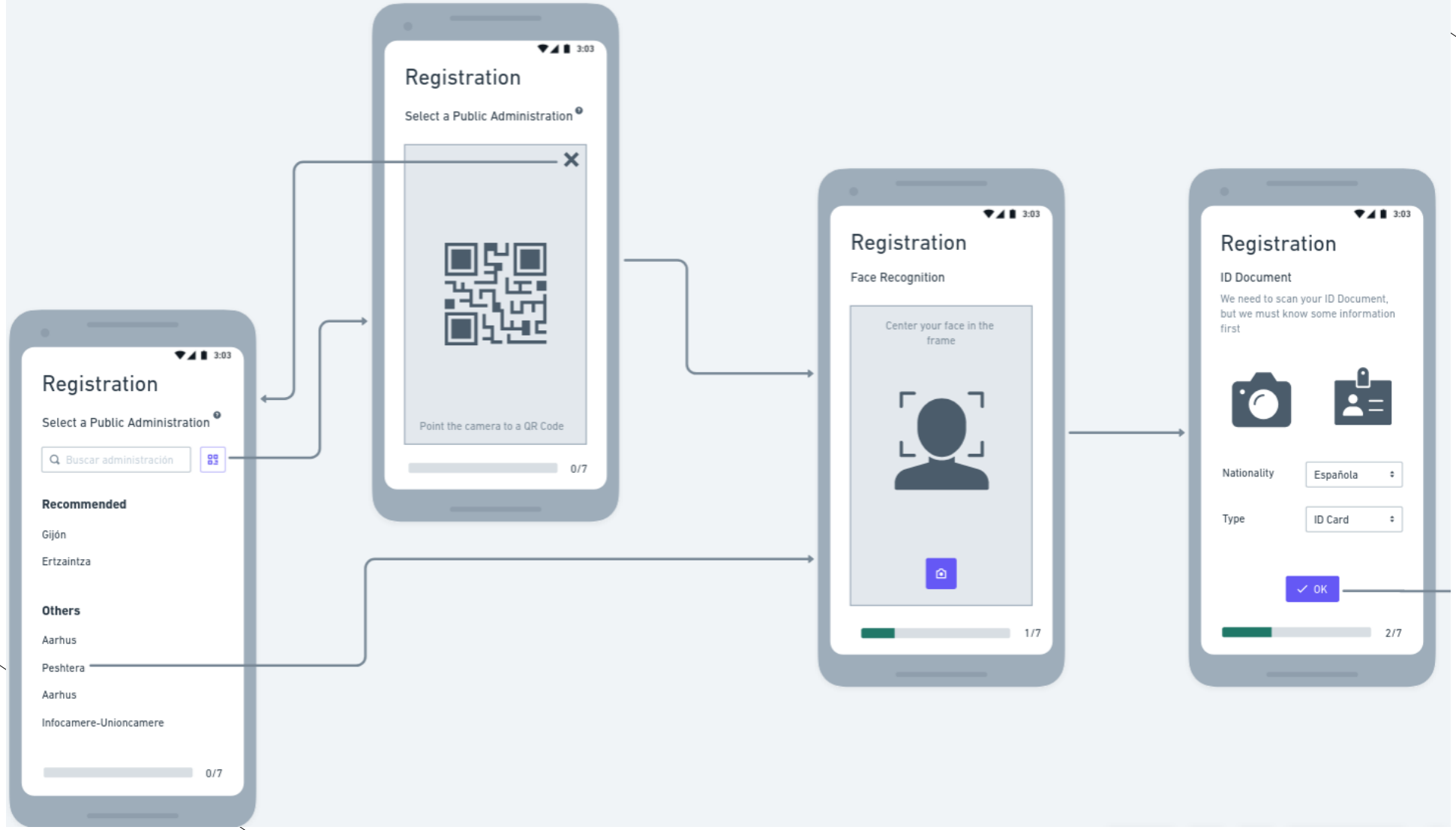


Processus d'authentification de l'utilisateur

Un utilisateur présente sa carte d'identité vérifiable pour être authentifié dans les services publics en ligne.

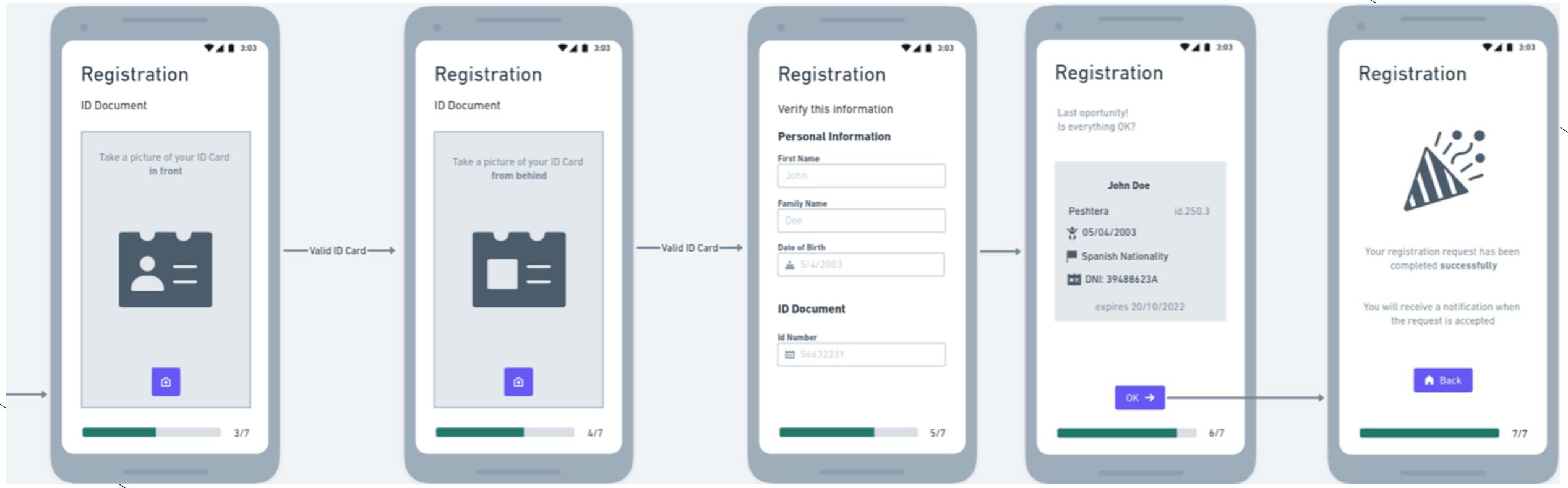
Impulse

Enregistrement **utilisateur**



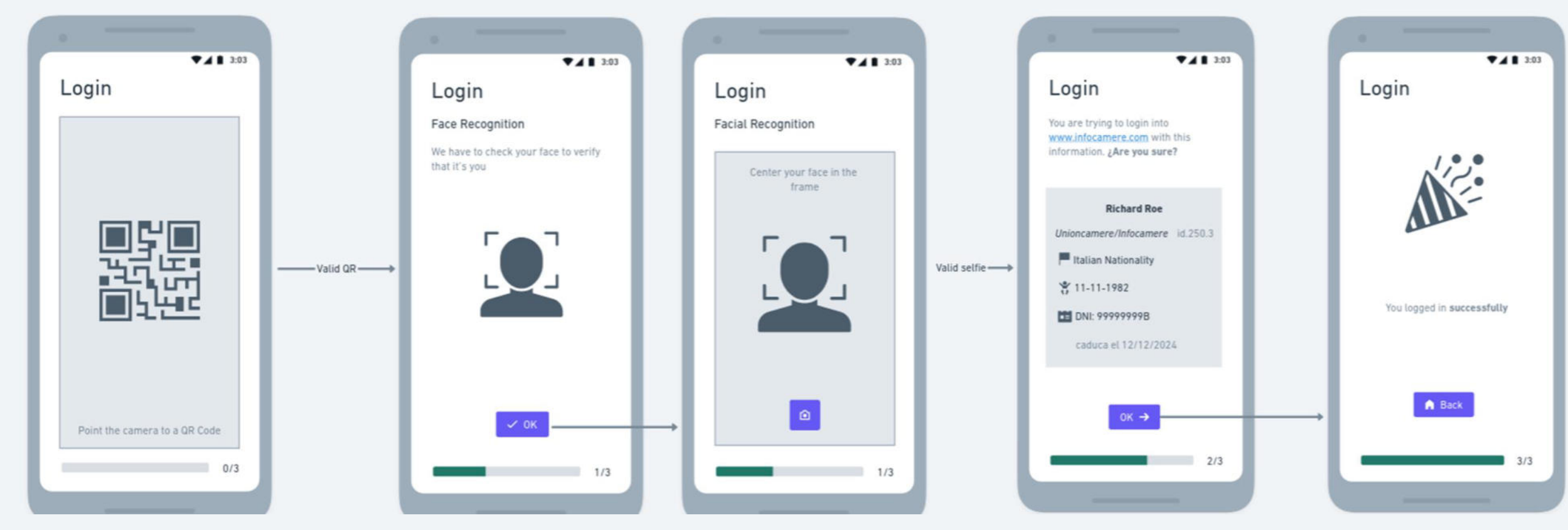
Impulse

Enregistrement **utilisateur**



Impulse

Authentification **utilisateur**



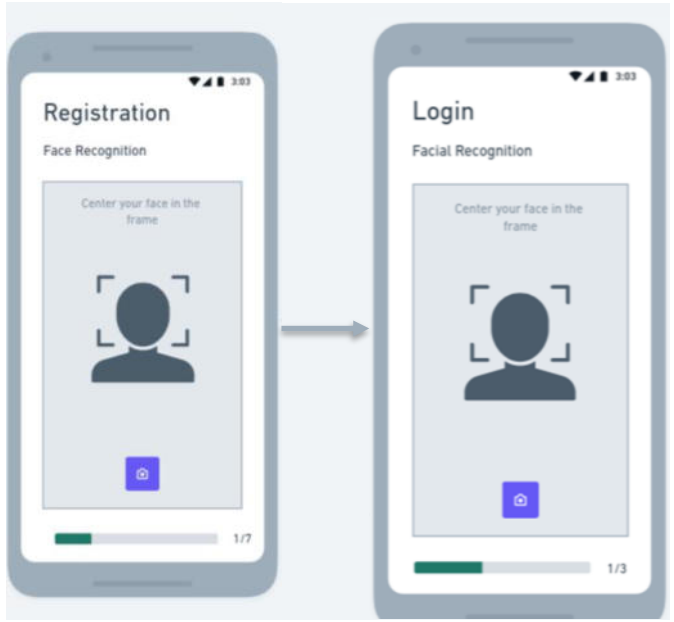
Impulse

Authentification **biométrique basée sur l'IA**

Le bloc technologique côté serveur (bloc serveur) est chargé de vérifier l'identité de l'utilisateur en utilisant son selfie et la photo du visage disponible dans son document d'identité. En outre, ce bloc effectue également une analyse de détection d'attaque de présentation (PAD) sur le selfie de l'utilisateur pour détecter d'éventuelles tentatives d'usurpation d'identité.

Le bloc technologique du dispositif mobile (bloc dispositif) permet à l'utilisateur d'être authentifié localement après son enregistrement dans la plateforme IMPULSE. Pour ce faire, en plus de l'acquisition vidéo, il expose deux fonctionnalités principales :

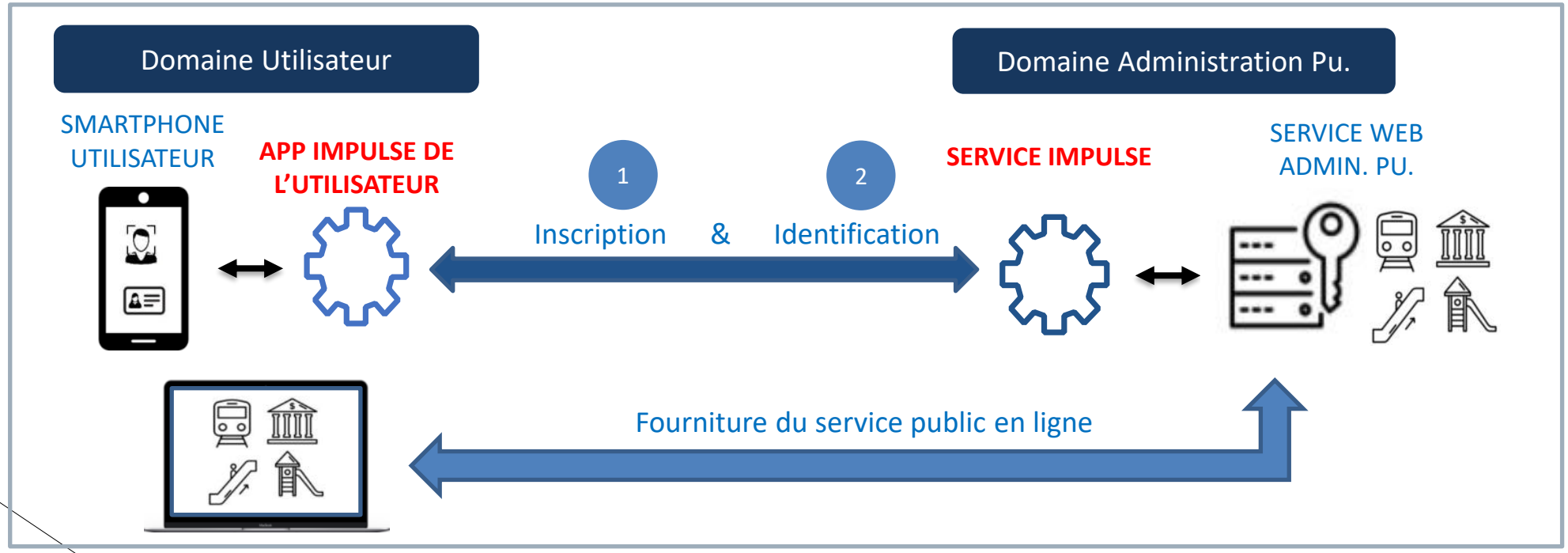
- **Extraction du profil du visage** : cette fonctionnalité génère un profil du visage de l'utilisateur à partir du selfie de l'utilisateur en effectuant également une analyse PAD similaire à celle du bloc serveur.
- **Comparaison des profils de visage** : ce module est chargé de comparer deux profils de visage d'utilisateur et de décider si les deux profils de visage appartiennent au même utilisateur ou non.



Impulse

IMPULSE **Intégration & Instanciation**

Les administrations publiques peuvent choisir n'importe quel service en ligne à intégrer au système de gestion de l'eID IMPULSE.



Impulse

Selon vous, quelles exigences techniques les solutions d'identité numérique comme IMPULSE doivent-elles remplir pour être adoptées par les municipalités et les services publics en général ?

Quid du secteur privé ?

En France, Belgique, Europe ?

Quels sont les principaux défis a relever pour répondre à ces exigences ?

Quelles sont vos préoccupations techniques concernant IMPULSE ?

Pour les municipalités, les services publics en général, le secteur privé ?

Impulse

Quels sont les autres systèmes d'identité électronique existant en France, belgique, Europe avec lesquels IMPULSE doit être interopérable ?

Quels sont les défis a relever dans ce domaine ?

Pour les municipalités, les services publics en général, le secteur privé ?

Impulse

Impulse

Identity Management in PUblic SErvices

Étude de cas
Méthodologie, besoins des utilisateurs, attentes des secteurs publics et privés

Facilitatrice : Marie PEREDA

Impulse

Cas **pilotes**

City of Reykjavík

Reykjavik, Iceland
Portail de participation démocratique *Better Reykjavik*

Aarhus, Denmark
Accès électronique aux informations et services personnels

Gijón, Spain
Public services app

Unioncamere & InfoCamere, Italy
Dossier numérique des entreprises

Ertaintza, Spain
Dépôt de plainte en ligne

Peshtera, Bulgaria
Enregistrement et certification de l'état civil

Impulse

Danemark – **Municipalité d'Aarhus**

Accès électronique aux informations et services personnels

Présentation
Actuellement, une carte (NemID) est nécessaire pour pouvoir accéder, par exemple, à sa boîte aux lettres numérique, sa banque, etc.. Les citoyens dit « vulnérables » (càd. SDF, en situation d'exclusion, etc.) ont soit perdu leur carte, soit l'ont stockée illégalement dans des centres d'hébergement. Il est nécessaire de trouver un accès et un stockage sécurisés des cartes-clés. La solution est la mise en place d'un casier / coffre-fort pour le stockage des papiers personnels, de santé, passeport (c'est-à-dire des éléments légaux et non des marchandises volées ou des drogues).

Type(s) de parties prenantes
- Refuges pour citoyens vulnérables
- Employés / bénévoles des refuges
- Fournisseurs tiers

Sujets d'intérêt à explorer/exploiter avec d'autres parties prenantes pour le bénéfice de la communauté locale
Le projet dépend des partenaires qui travaillent en étroite collaboration avec les citoyens vulnérables, ainsi que des personnes travaillant dans des centres d'hébergement ou des municipalités / organisations qui expérimentent de tels casiers.

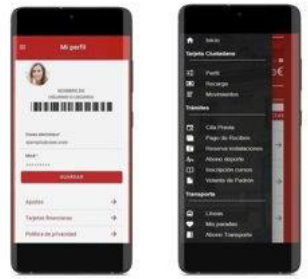
Impulse

Espagne – **Municipalité de Gijon**

Carte de citoyen pour la participation à la gouvernance électronique (vote électronique).

Présentation

La Citizen Card est le principal outil utilisé par les citoyens de Gijón, notamment pour l'utilisation des services de transports, de réservation, de billetterie, etc.. Cependant, les méthodes de vérification de l'identité présentent des faiblesses (images floues, textes détériorés, codes compliqués à mémoriser, etc.) qui limitent son utilisation.



Type(s) de parties prenantes

- Municipalité et ses services liés
- Citoyens
- Acteurs externes intéressés pour figurer sur l'app (ex. cinéma, boutiques, etc.)

Sujets d'intérêt à explorer/exploiter avec d'autres parties prenantes pour le bénéfice de la communauté locale

L'idée serait d'inclure la possibilité d'utiliser la City Card pour voter afin d'assurer la participation des citoyens à la gestion de leur ville. Développer l'utilisation de l'IA et des données biométriques (visage, doigt, yeux) pour disposer réellement d'un outil sans contact rapide.

Espagne – **Dép.de police du Pays Basque**

Déposer une plainte entièrement en ligne

Présentation

A l'heure actuelle pour déposer une plainte, il est possible de le faire sur le site www.ertzaintza.euskadi.eus en remplissant toutes les informations requises. Cependant, ensuite la procédure requiert la confirmation et la signature de la plainte déposée au plus tard dans les 72 heures en se rendant dans un commissariat de police. Avec une solution d'identification biométrique telle qu'IMPULSE, Le processus se termine par l'identification directe du plaignant en ligne, accélérant ainsi le processus de traitement et réduisant les déplacements.

Type(s) de parties prenantes

- Poste de police et agents de police
- Citoyens

Sujets d'intérêt à explorer/exploiter avec d'autres parties prenantes pour le bénéfice de la communauté locale

L'idée serait de se servir de ce cas spécifique, traitant de données parfois très sensibles comme exemple. Notamment pour des institutions juridiques, des banques, des zones à accès restreints, etc.

Impulse

Bulgarie – **Municipalité de Pestera**

Registre électronique / Portails de démocratie participative de Reykjavik et e-Reykjavik

Présentation

La municipalité a récemment lancé une plateforme de services numériques et offre environ 70 services publics à ses citoyens, mais le nombre d'utilisateurs est assez faible. Les citoyens préfèrent les visites physiques "au comptoir", plutôt que les services numériques en ligne. Ceci vient aussi de méfiance envers les méthodes d'identification et le partage des données en ligne (récent cas de fuites de données)

Type(s) de parties prenantes

- Municipalité et ses services liés
- Citoyens

Sujets d'intérêt à explorer/exploiter avec d'autres parties prenantes pour le bénéfice de la communauté locale

L'idée est d'utiliser ce cas comme un exemple pour montrer la possibilité d'accroître la confiance des citoyens dans l'utilisation des services numériques et de multiplier les moyens (sécurisés) de se connecter à la plateforme de services. Mais aussi la sensibilisation des citoyens à la solution d'identification électronique, aux technologies, aux services numériques, etc. afin d'assurer la confiance dans ce type d'identification, d'inverser la crainte de fuite de données et d'augmenter le niveau d'alphabétisation électronique (en particulier chez les personnes âgées et/ou les groupes cibles vulnérables comme les personnes à faible revenu, les personnes ayant un faible niveau d'éducation, etc.

Impulse

City of Reykjavík

Islande – **Municipalité de Reykjavik**

Enregistrement et certification de l'état civil

Présentation

Electronic Reykjavik est une initiative récente visant à créer de nouveaux services numériques entre les citoyens et la ville de Reykjavik. L'ambition est de faciliter et de sécuriser l'accès aux portails de services de Reykjavik afin qu'aucun citoyen ne soit laissé pour compte dans la transformation numérique de Reykjavik.

Type(s) de parties prenantes

- Municipalité et ses services liés
- Citoyens (focus sur les personnes vulnérables)

Sujets d'intérêt à explorer/exploiter avec d'autres parties prenantes pour le bénéfice de la communauté locale

L'idée est d'utiliser ce cas comme un exemple d'une municipalité déjà très avancée dans sa transformation digitale et qui ainsi, a pu se rendre compte que malgré les bénéfices du numérique, des problèmes ont pu émerger. Notamment l'usage par les personnes plus âgées, celles avec un handicap physique ou mental, etc. Et comment une solution telle qu'IMPULSE pourrait aider, ou non, à contrer ce genre de problématiques.

Impulse

Italie – **Chambre de commerce**

Propriétaire d'entreprise - Identités légales

Présentation

A l’heure actuelle, le parcours administratif auprès de la chambre de commerce, pour les entreprises, est complexe et long. De plus, de la fraude et de la fausse comptabilité sont souvent constatés. Avec IMPULSE, les entrepreneurs peuvent accéder au "tiroir numérique" pour vérifier, télécharger et partager des données, des certifications, le profil de l'entreprise, des états financiers, l'état des demandes adressées à l'administration publique, des factures numériques, etc. Et l’administration peut vérifier de son côté la régularités des pièces.

Type(s) de parties prenantes

- Chambres de commerce
- Entrepreneurs

Sujets d'intérêt à explorer/exploiter avec d'autres parties prenantes pour le bénéfice de la communauté locale

Cette étude de cas diffère des autres car elle touche aussi au secteur privé. Elle permet ainsi de faire le lien avec ce dernier vis-à-vis de la solution développée et donc de permettre l’exploration d’autres usages par le secteur privée de cette solution.

1ere itération des **cas pilotes**

- **Défis techniques lors de la mise en place de la solution IMPULSE sur les sites de cas**
- **L'onboarding a été un peu lourd**
- **Manque d'informations si quelque chose fonctionne ou échoue**
- **Pas de politique de confidentialité ou d'information sur le stockage des données**
- **Certaines parties de l'application étaient confuses**
- **Que se passe-t-il si les caméras ne fonctionnent pas correctement ou ne sont pas assez bonnes (mauvaise qualité d'image) ?**

- **La majorité a perçu la reconnaissance faciale comme sûre et digne de confiance, ainsi que plus facile et plus sûre que les autres identifications biométriques.**
- **L'identification est rapide et la solution est facile à utiliser.**
- **La solution constitue une bonne (ou meilleure) alternative aux systèmes actuellement en place et la plupart l'utiliseraient à l'avenir après des améliorations techniques.**
- **Dans l'ensemble, la solution est considérée comme sûre (avec quelques réserves).**

Impulse

Quels sont les principaux cas d'utilisation des solutions d'identité numérique pour les municipalités, les services publics en général, et le secteur privé ?

En France, Belgique, Europe ?

Impulse

Quelles sont les principales exigences que les solutions d'identité numérique, comme IMPULSE, doivent satisfaire pour être largement adoptées ?

Pour les municipalités, les services publics en général et le secteur privé ?

Impulse

Quels sont les principaux défis à l'adoption de nouvelles solutions d'identité numérique, comme IMPULSE, pour les municipalités, les services publics en général et le secteur privé ?

En France, Belgique, en Europe ?

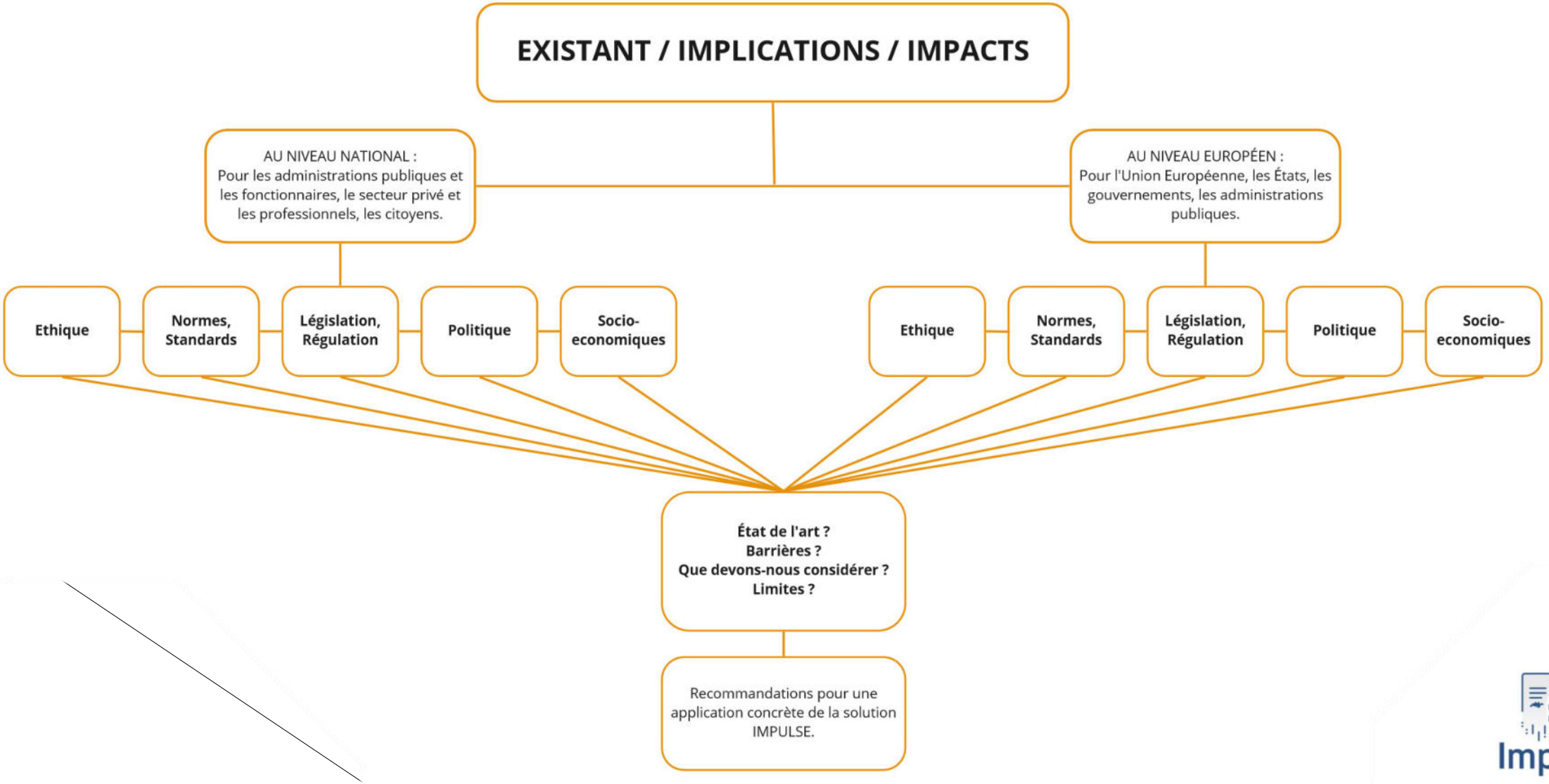
Impulse

Identity Management in PUblic SErvices

Impact du développement des solutions eID
Réglementations, normes, éthique, législation et droit

Facilitateur : Benjamin CHERET

L’approche **eID d’IMPULSE**



Impulse

Quelles sont les principales exigences légales, réglementaires, éthiques, sociales, etc. auxquelles une solution d'identité numérique, comme IMPULSE, doit répondre ?

Lesquelles de ces exigences sont généralement les plus difficiles à satisfaire ?

Impulse

Selon vous, est ce qu'une identité digitale basé sur la reconnaissance biométrique pourrait être utilisée comme signature électronique qualifiée (QSeal) ?

En France, en Belgique, en Europe ?

Impulse

Que peut faire l'Etat et/ou la Commission Européenne pour soutenir la diffusion des solutions d'identité numérique en France, en Belgique, en Europe ?

Existe-t-il des lois / directives à l'heure actuelle ?

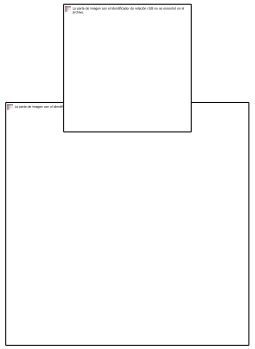
Impulse

Retour à la session principale

Impulse

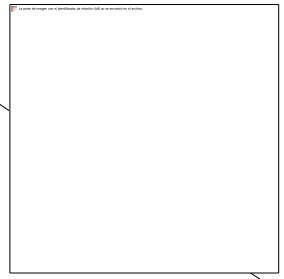
Et **maintenant ?**

Réunions thématiques



Organisation de tables rondes thématiques sur les sujets IMPULSE avec les membres du consortium concernés, à l'invitation du projet ou à votre suggestion. Les tables rondes servent également à la mise en réseau et à la collaboration.

Enquête en ligne



Enquête pour mieux comprendre les usages, les besoins, les intérêts et l'appréciation des utilisateurs, de tous types et de toutes nationalités, pour une solution d'identification électronique telle que nous la développons.

Impulse

Contactez-**nous**

E-mail

bertille.auvray@pole-tes.com

Website

www.impulse-h2020.eu

Social Media

Twitter: @Impulse_EU
LinkedIn: @IMPULSE project H2020

Merci pour votre participation

Impulse

Identity Management in PUbLic SErvices

Online Workshop

Smartphone-based digital identities using facial recognition for public services

IMPULSE solution, use cases, adoption requirements

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

Impulse

Agenda

1. **Welcome and Introduction of the IMPULSE Team**
2. **Overview IMPULSE: Project, Technology and Use Cases**
3. **Q & A**
4. **Break-out sessions: Possibilities and Constraints for Adoption in Denmark, Iceland and Finland**

Audio/Video recording:

We kindly ask for your permission to record the workshop
... but you may of course refuse!

Access to recordings will be strictly limited to IMPULSE team members

Recordings will be only used for research and documentation purposes

Recordings will be erased at the latest after project end in January 2024

Impulse

Agenda

1. **Welcome and Introduction of the IMPULSE Team**
2. **Overview IMPULSE: Project, Technology and Use Cases**
3. **Q & A**
4. **Break-out sessions: Possibilities and Constraints for Adopting IMPULSE in local environments**

Impulse

Agenda

1. Welcome and Introduction of the IMPULSE Team
2. Overview IMPULSE: Project, Technology and Use Cases
3. Q & A
4. Break-out sessions: Possibilities and Constraints for Adopting IMPULSE in local environments

Impulse

Identity **M**anagement in **PU**blic **SE**rvices

General presentation of the project

Impulse

Who we are

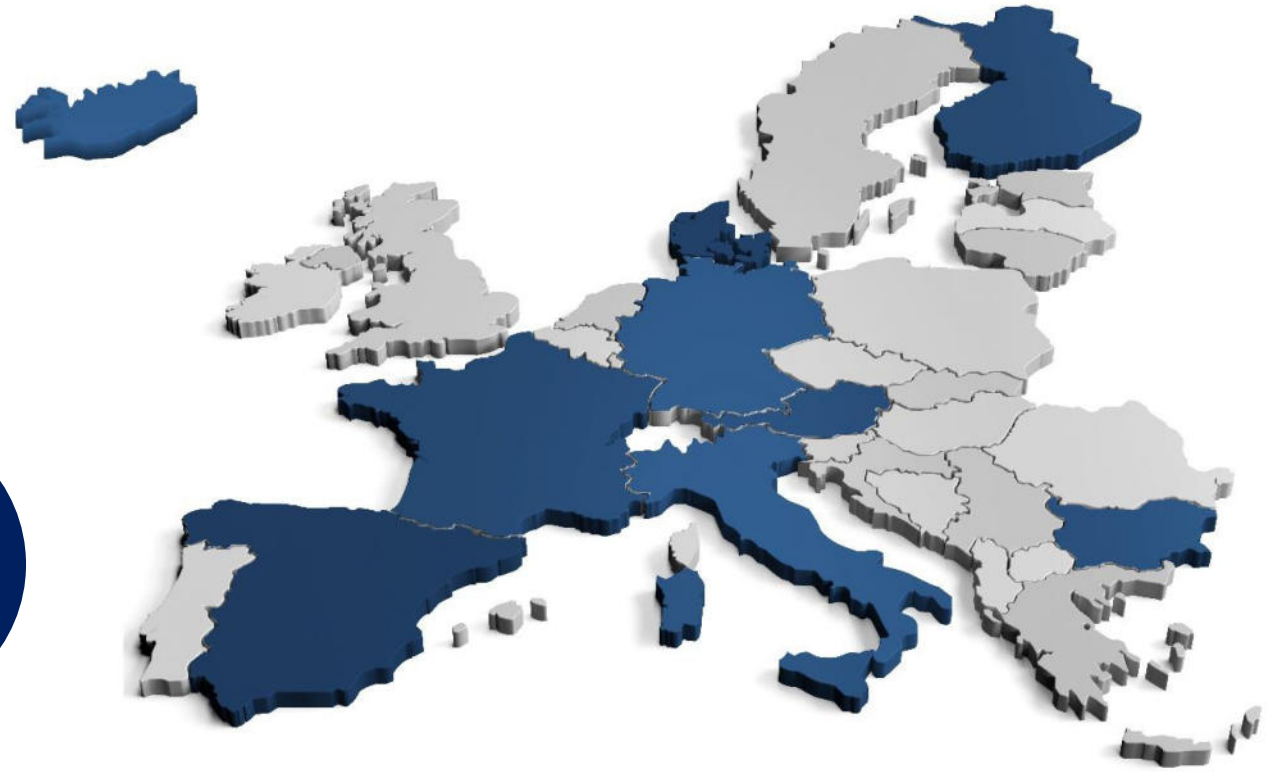
HORIZON 2020

LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

2021
2024

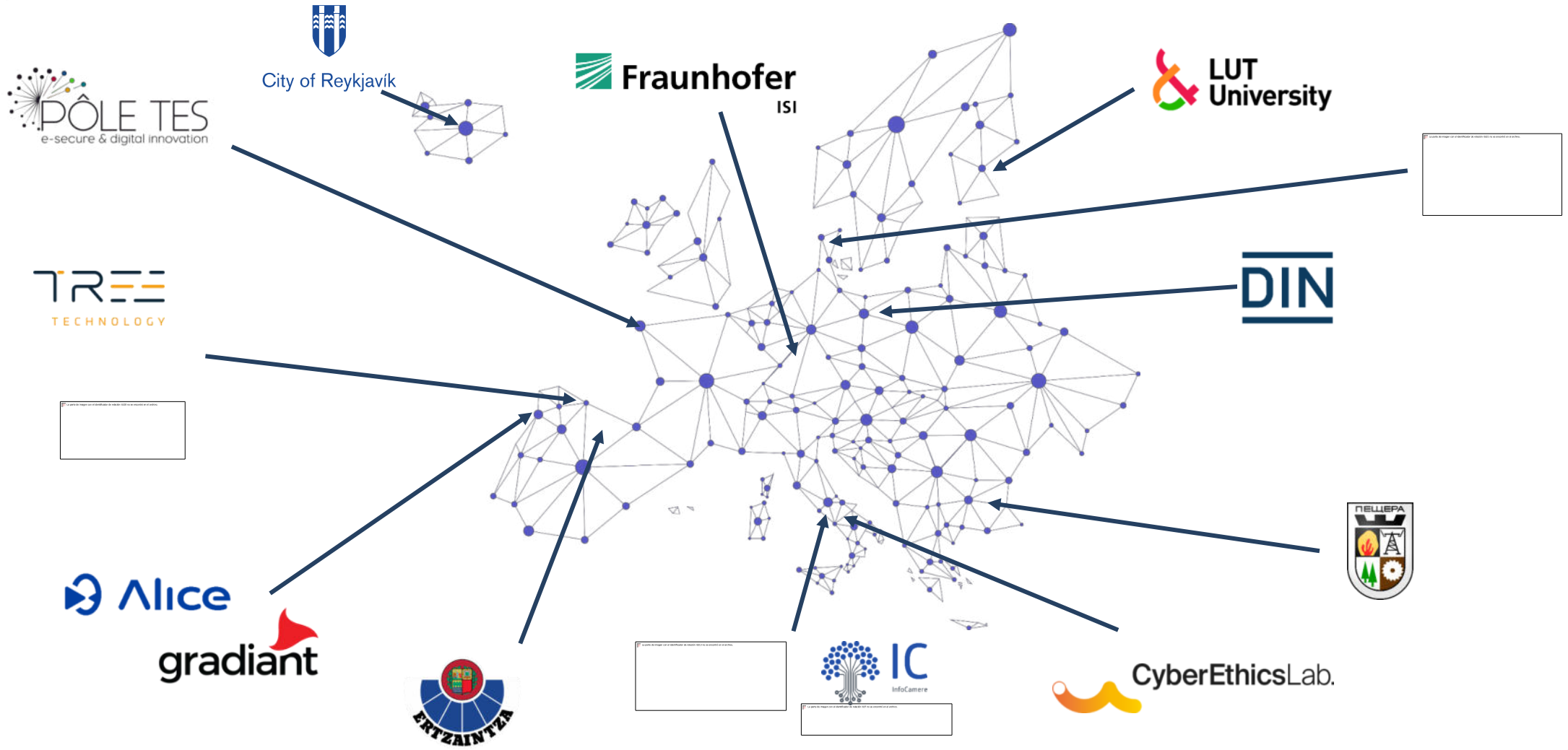
15 partners

+3M€



Impulse

The consortium



Impulse

Project Objectives

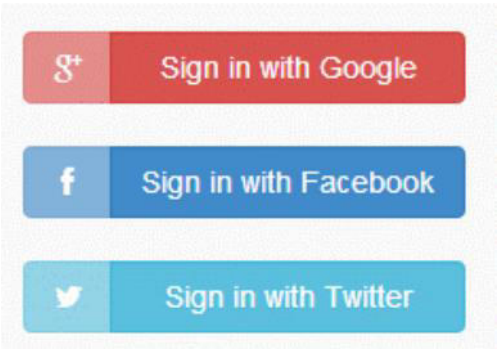
- Develop a **decentralised**, **self-sovereign digital identity management system** that uses **facial recognition** to authenticate the user
- **Trial** the system in **6 public service use cases** across Europe
- Evaluate **impact**, support **regulatory** and **standardisation efforts**
- Develop **roadmaps** for possible future **real-world deployments** of the system
- **Aim by Project End**: reach **TRL 6** (prototype system)
  - Options **Post-Project**: develop IMPULSE to **TRL 9** (commercialisation) or **re-use individual components** of the IMPULSE system in new solutions, possibly with new partners

Overview of IMPULSE – Electronic Identity Systems

- Traditional eID management systems are based on centralized architectures

  - **User ID and password**
    - ✓ Centralized identifiers
    - ✓ Many passwords to track

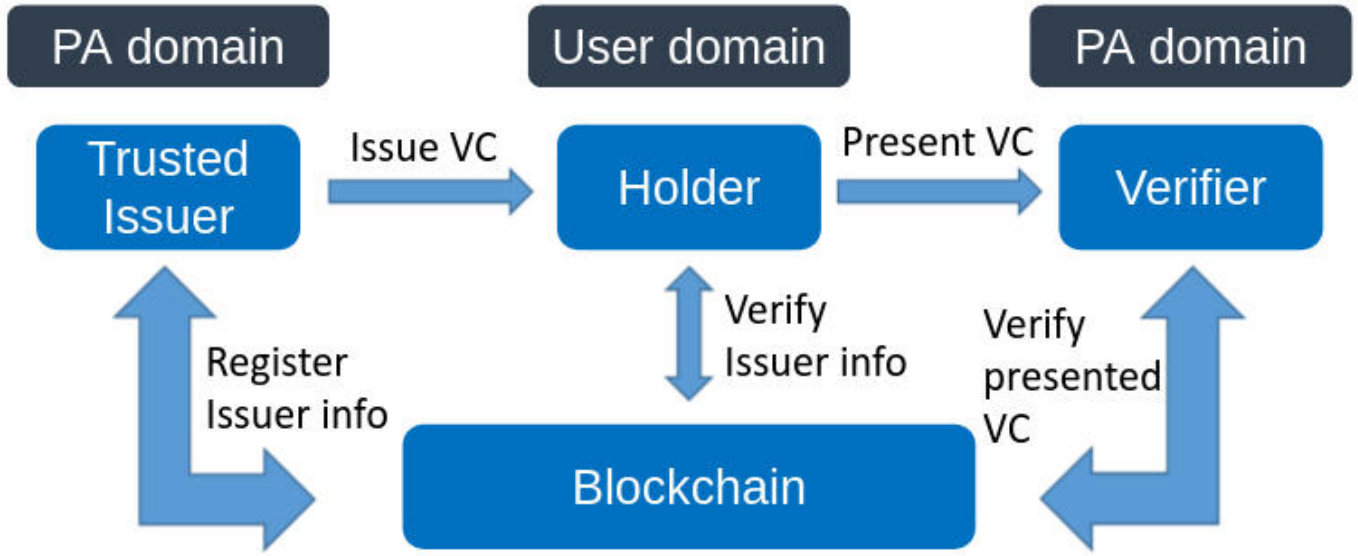
  - **Identity Providers (IdPs)**
    - Only one password but…
    - Identities are controlled by an unique third party -> IdP
    - IdPs learns things about us -> habits, interests
    - Unwanted Correlations



  - **User Certificates (PKI)**
    - Good but...
    - They are not very respectful of user privacy
    - Installation process is complex for the average user
    - Centralized root of trust

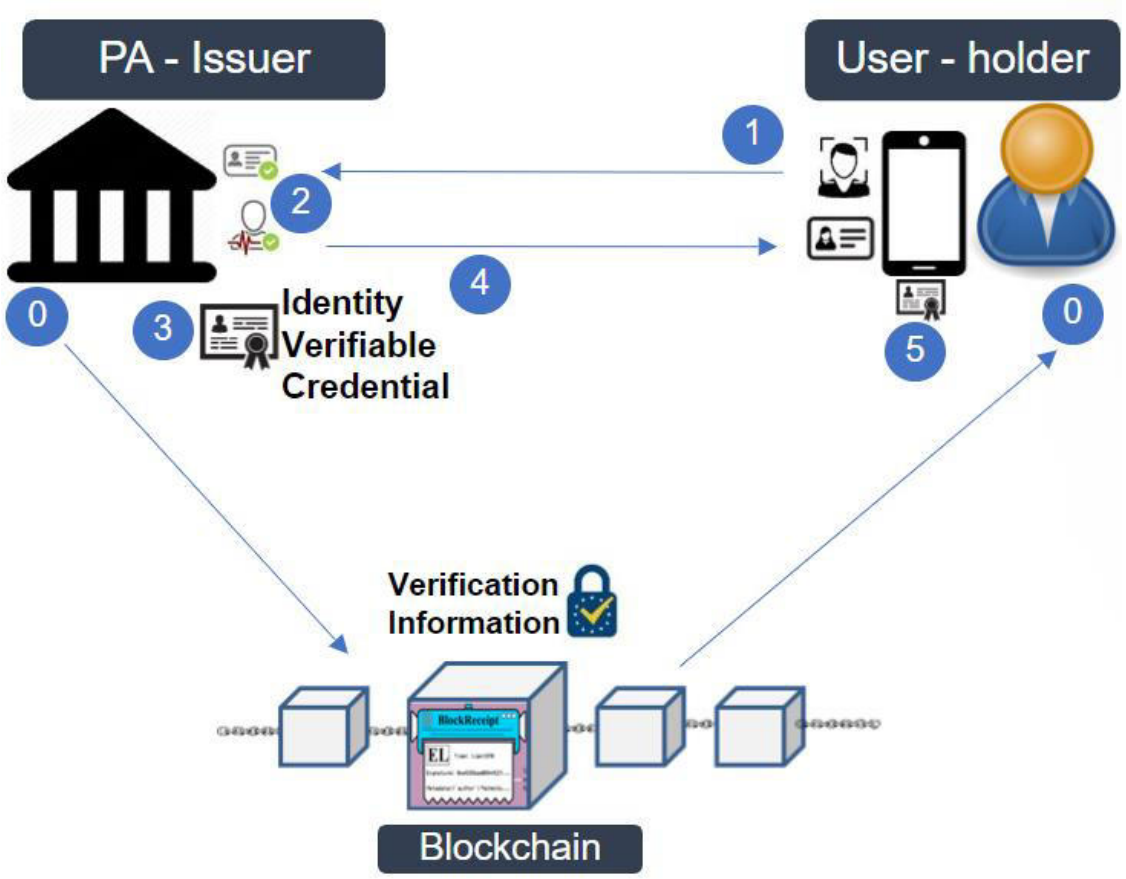
Overview – IMPULSE as an alternative eID System

- IMPULSE intends to **solve the centralized eID system issues**
- IMPULSE proposes a **decentralized** and **self-sovereign** eID management system based on a **verifiable credential** (VC) model upon **blockchain**



Impulse

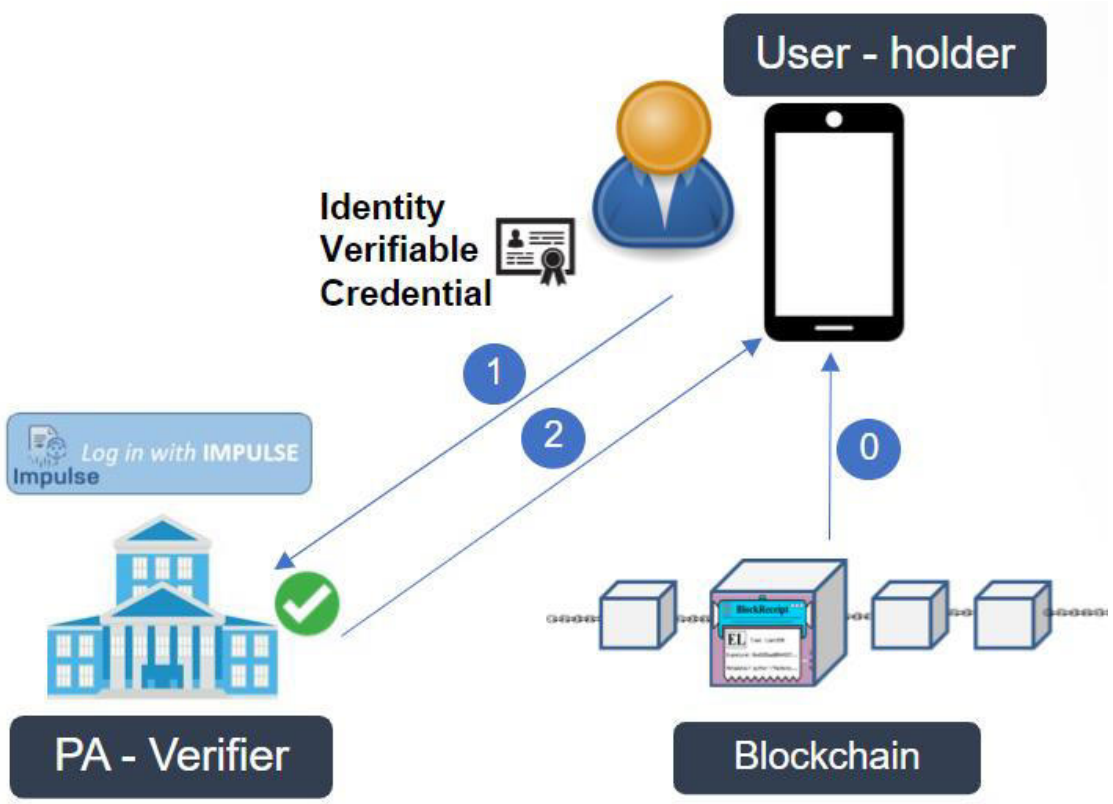
Overview – User Registration



[0] Verification information (public keys) are stored on the Blockchain

1. User takes a selfie and a photo of their ID document (ID card, passport)
2. IMPULSE system uses AI to
   - check correlation btw selfie & ID photo
   - verify ID document
   - extract data from ID doc (name, etc)
3. IMPULSE system issues user with an Identity Verifiable Credential
4. Verifiable Credential is securely stored in the user's device
5. Verification information inscribed on blockchain

Overview – User Authentication



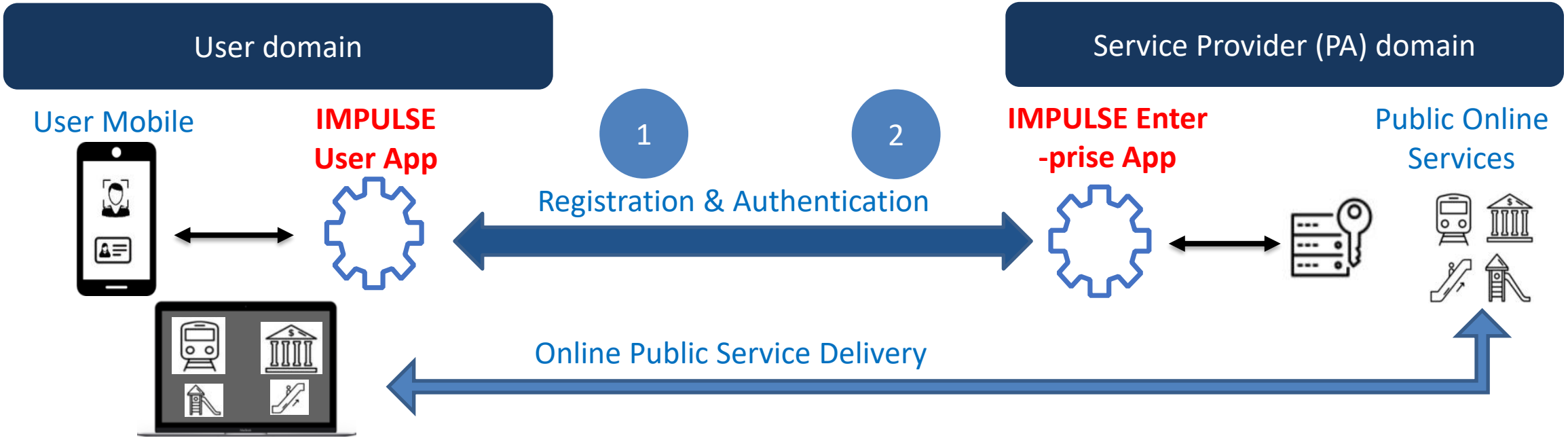
[0] User goes to PA website, chooses “Log in with IMPULSE”

[0] IMPULSE App opens and recovers verification information from the blockchain

1. User takes a selfie to authenticate to IMPULSE;
2. IMPULSE App presents the Verifiable Credential stored on the device to the PA
3. The PA confirms the Verifiable Credential and delivers the requested service to the User

Overview – Integration & Instantiation

- Any online service can be integrated with the IMPULSE Digital Identity Management System
- → Install IMPULSE Android App (Google PlayStore) (User), deploy Container (Service Provider)
- IMPULSE is based on EBSI/ESSIF ecosystem & EBSI Identity Verifiable Credential Schema



Overview of IMPULSE – Planned Improvements

- **Trusted Execution Environments:** for the Wallets in the User Application and the Enterprise Application
- **Remote QSeal Service:** Identity Credentials signed with a qualified signature
- **Informed Consent Service:** Management of the user consent by sharing data through Smart Contracts

IMPULSE Project: 6 Pilots

Impulse

City of Reykjavík

Reykjavik, Iceland
Better Reykjavik participatory democracy portal

Aarhus, Denmark
Electronic access to personal information and services

Gijón, Spain
Public services app

Unioncamere & InfoCamere, Italy
Enterprise digital drawer

Ertaintza, Spain
Issuing complaints entirely online

Peshtera, Bulgaria
Civil registration & certification

General Feedback from Pilots

First "live" tests of the IMPULE App with local citizens in Sept.-Oct. 2022 across the 6 Pilots

- Generally positive feedback...
  - 65% would be "likely"/"very likely" use IMPULSE, 71% would recommend it to others
  - No passwords!
  - Fast and simplified access to online services
  - Generally positive associations (convenient, time saving, safe, useful etc)
- ...But some improvements still necessary
  - In some cases, onboarding process insufficiently clear and users needed help
  - Notifications can still be improved
- Feedback now being analysed to further improve IMPULSE

IMPULSE in Aarhus, Denmark

Aarhus' Challenge: Secure storage for homeless people

Impulse

Status Quo:

- Homeless people and people living in unstable situations often lack a place to securely store documents and other valuables (e.g. NemID cards)
- Conventional lockers with keys or PINs provide limited help: Keys must also be stored securely; PINs are easily forgotten

Consequence:

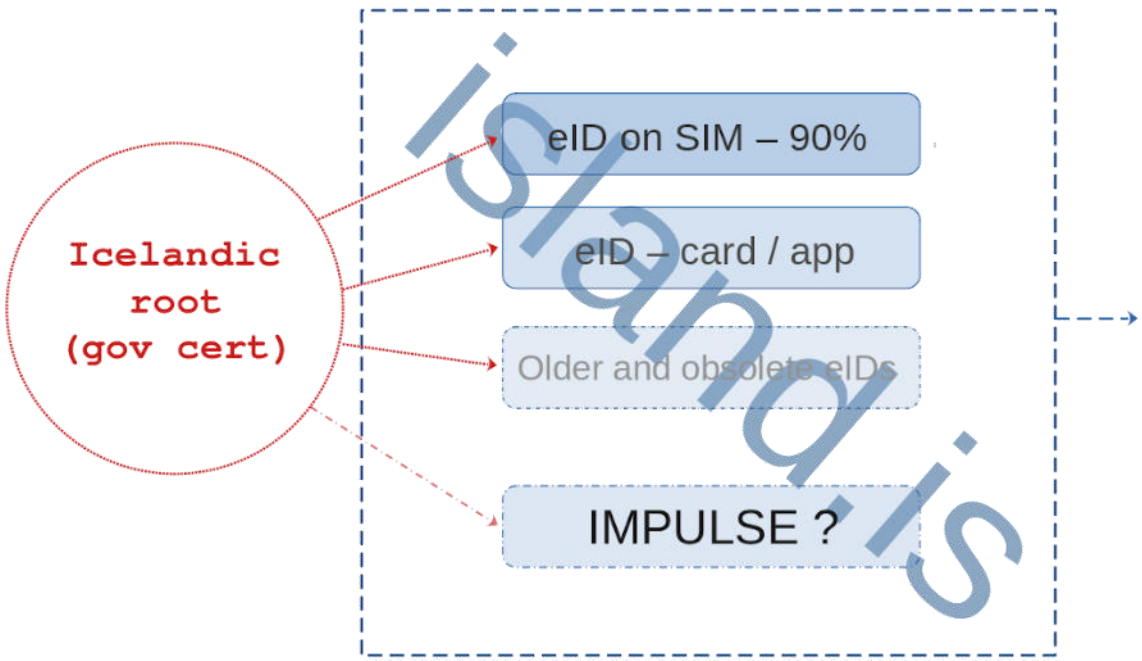
- Vulnerable individuals often lose important documents
- Additional work/cost for social services staff

How can IMPULSE help?

- Lockers using the IMPULSE facial recognition and identity management technology:
  - Secure document storage
  - Easily accessible
  - No physical keys or passwords / PINs needed

IMPULSE
biometric recognition for physically impaired people

Advantages of biometric recognition ?



Online services, requiring proof of identity

Customers of the FidM	Total	%	Notes
Municipalities	28	10.65%	*public services*
National government institutions	32	12.17%	*public services*, including the healthcare hub (VERA) and government insurances (e.g. health, natural disaster, pension, disability)
Apotheke	1	0.38%	private pharma
Pension Funds	19	7.22%	public and private
Companies (commercial / non-profit)	23	8.75%	varied - e.g. energy companies, animal registry and employment / tax filing services
Extracurricular support	62	23.57%	organisations, offering concessions (through govt & non-profit org) to membership in sports and other organised youth and adult activities
Junior colleges	32	12.17%	used to access online learning, records and resources
Financial institutions	23	8.75%	banks, investors, insurance companies, credit, lotto, collectors
Other agencies	43	16.35%	varied - a lot of employee organisations and unions
Total	263	100.00%	

Advantages of biometric recognition ?

Understanding the mandate:

- The cases in which it is an absolute requirement that a person can prove they are who they say they are.
  - Has facial recognition reached the maturity to pass certification for official purposes?

- The (other types of) cases in which facial recognition protocol like IMPULSE can thrive

The future environment to consider:

- Participation in Europe-wide developments in giving out official electronic IDs and in document handling
  - The EU blockchain, EBSI
  - A new standard, now underway eIDAS2 and certificates (QWAC and QSEAL)
  - How is the issuing of electronic identity handled

Agenda

1. Welcome and Introduction of the IMPULSE Team
2. Overview IMPULSE: Project, Technology and Use Cases
3. Q & A
4. Break-out sessions: Possibilities and Constraints for Adopting IMPULSE in local environments

Questions & Answers

Impulse

Agenda

1. **Welcome and Introduction of the IMPULSE Team**
2. **Overview IMPULSE: Project, Technology and Use Cases**
3. **Q & A**
4. **Break-out sessions: Possibilities and Constraints for Adopting IMPULSE in local environments**
   - Use Cases
   - Technology
   - Law and Regulation

Impulse

Break-out

IMPULSE i en dansk kontekst

Potentialer ved IMPULSE

I dine øjne...

- **Er der fordele ved at have flere tilgængelige eID-løsninger i en dansk kontekst?**
  - **Hvilke fordele? Hvornår?**
  - **Hvad er hovedudfordringerne ved at have flere tilgængelige eID-løsninger?**

- Kommunalt / Regionalt?
- Statsligt?
- I den private sektor?

Biometriske og teknologiske krav

I dine øjne...

- **Vil biometrisk login øge datasikkerheden?**
- **Vil biometrisk login øge tilgængeligheden af digitale services?**
- **Hvilke fordele/ulemper kan biometrisk login have for forskellige målgrupper**

- Kommunalt / Regionalt?
- Statsligt?
- I den private sektor?

Impulse

Discussion

Options for IMPULSE in Iceland and Finland

Benefits and Use Cases

In your view...

- **Are there benefits from having multiple eID solutions in the Icelandic and Finnish context?**
  - **In what use cases might IMPULSE add value in Iceland and Finland?**
  - **What are the main challenges to adopting IMPULSE in Iceland and Finland?**

- **In Municipalities?**
- **In Central Government?**
- **In the Private Sector?**

Biometrics and Technology Requirements

In your view...

- **Will biometric login increase data security and accessibility for vulnerable people?**
- **What technical requirements must IMPULSE meet to be adopted? What are key challenges to meeting these?**
- **What interoperability requirements are there for IMPULSE?**

- In Municipalities?
- In Central Government?
- In the Private Sector?

Law, Regulation and Policy

In your view...

- **What are the main legal and regulatory requirements that a digital identity solution like IMPULSE must meet, including certifications?**
- **Which of these requirements tend to be hardest to meet?**

Next Steps in the IMPULSE Project

- 2nd Iteration of the IMPULSE system and Piloting
- Complete impact assessment work
- Further workshops in other pilot countries
- Develop country-specific roadmaps

Identity Management in PUbLic SErvices

Jakob Asmussen jaas@aarhus.dk

Kristrún Gunnarsdóttir Kristrun.Gunnarsdottir@Reykjavik.is

Jiri Musto Jiri.Musto@lut.fi

Javier Gutiérrez Meana javier.gutierrez@treetk.com

Jaime Loureiro Acuna jloureiro@gradiant.org

Nicholas Martin nicholas.martin@isi.fraunhofer.de

Thank you!

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

Impulse

Identity Management in PUbLic SErvices

InfoCamere
Innovare è Crescere

Intelligenza artificiale e blockchain nell'app IMPULSE e confronto con il sistema di identità digitale SPID

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

Impulse

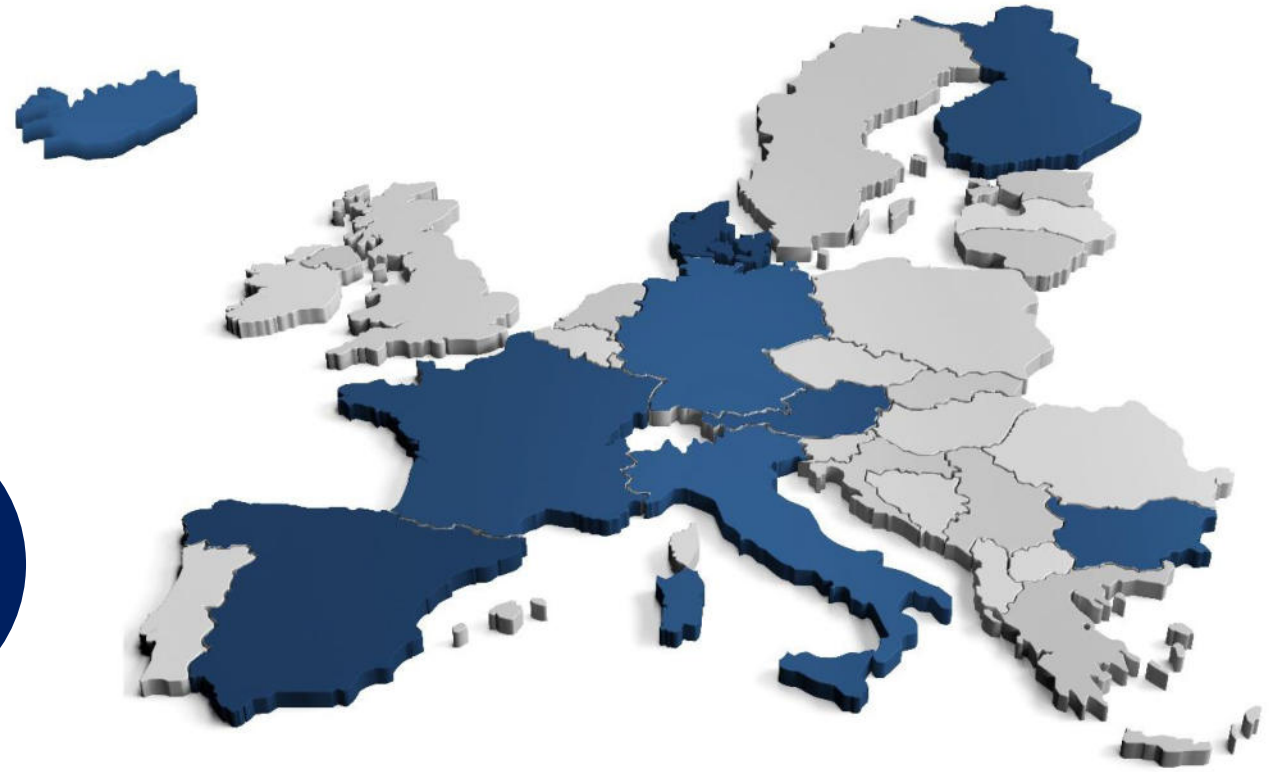
Chi siamo

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

2021
2024

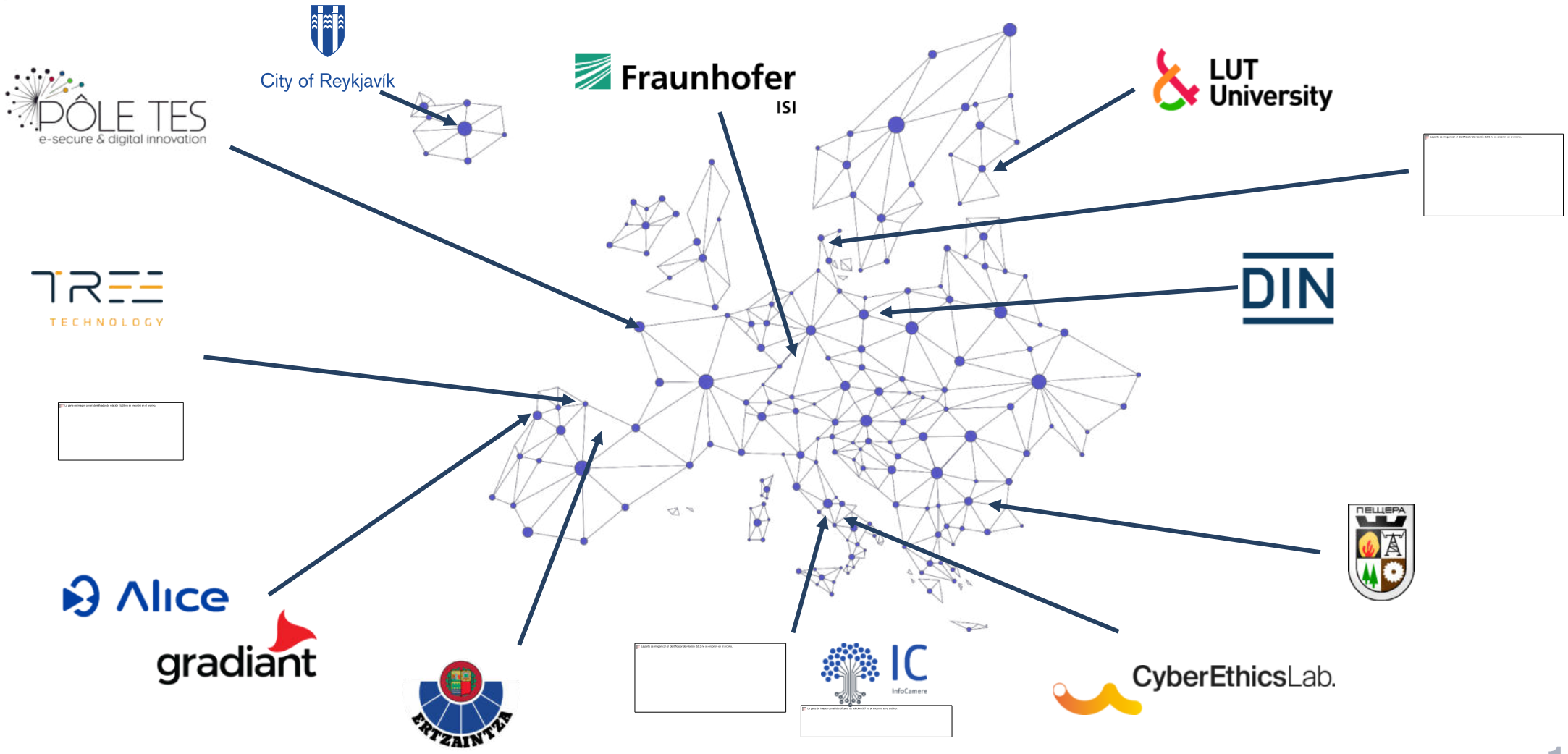
15 partners

+3M€



IMPULSE - Identity Management in PUbLic SErvices

Il consorzio IMPULSE



Impulse

Obiettivi del progetto

- La sperimentazione di tecnologie cosiddette "dirompenti" (disruptive) in processi e servizi pubblici (intelligenza artificiale, blockchain).
  - Livello di Maturità Tecnologica entro la fine del progetto: TRL 6
  - Possibile sviluppo dopo la chiusura del progetto: TRL 9
- 6 pilot
- Impatto sociale, economico, legislative e possibile standardizzazione
- Roadmaps futura

IMPULSE Project: 6 Pilots

Impulse

City of Reykjavík

Reykjavik, Iceland
Better Reykjavik participatory democracy portal

Aarhus, Denmark
Electronic access to personal information and services

Gijón, Spain
Public services app

Unioncamere & InfoCamere, Italy
Enterprise digital drawer

Ertaintza, Spain
Issuing complaints entirely online

Peshtera, Bulgaria
Civil registration & certification

Use Cases

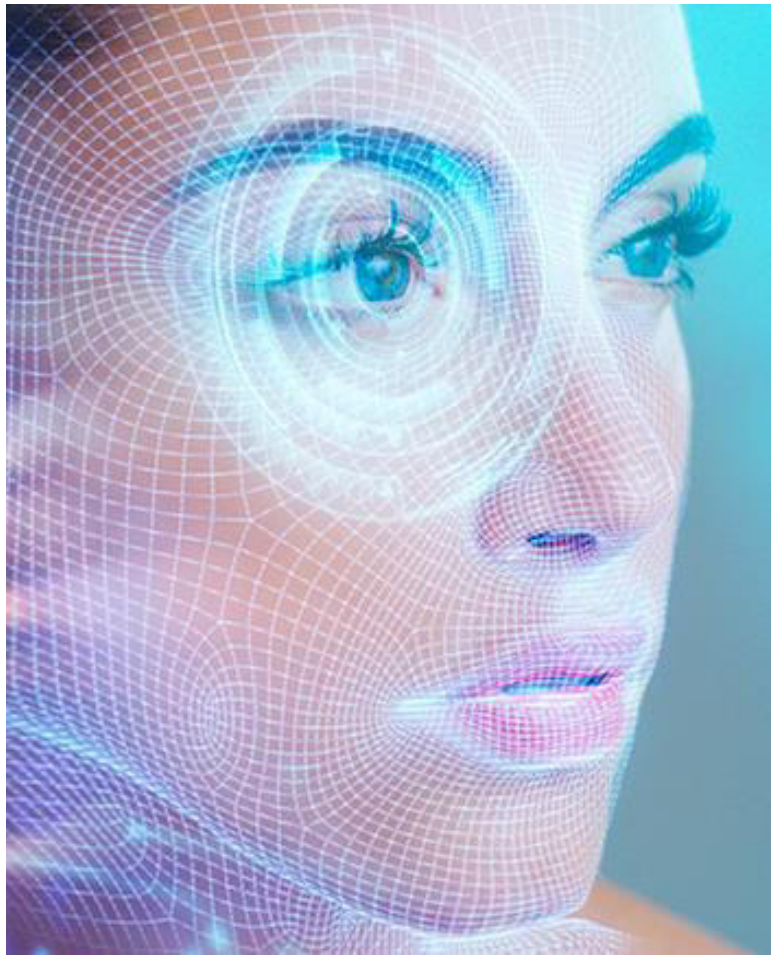
- **Dove può essere utilizzata l'identità digitale? (Settore pubblico, privato, ecc)**
- **Quali sfide/difficoltà comporta l'adozione dell'identità digitale in Italia?**
- **Quali sono i timori e i dubbi principali nell'adottare l'identità digitale? (privacy, dati, ecc)**

Overview of IMPULSE – Intelligenza Artificiale

L'intelligenza artificiale (IA) entra in gioco nella tecnologie usate da IMPULSE attraverso l'utilizzo di algoritmi di apprendimento automatico.

Questi algoritmi consentono alla tecnologia di **apprendere** da un grande numero di esempi di volti e documenti e di migliorare continuamente la sua capacità di riconoscere e identificare i volti e i documenti degli utenti.

In altre parole, l'IA consente alla **tecnologia** di diventare **sempre più precisa e affidabile** nel riconoscimento dei volti e dei documenti, anche in condizioni difficili (illuminazione o di posizione della testa) al punto di diventare più preciso di un controllo umano.

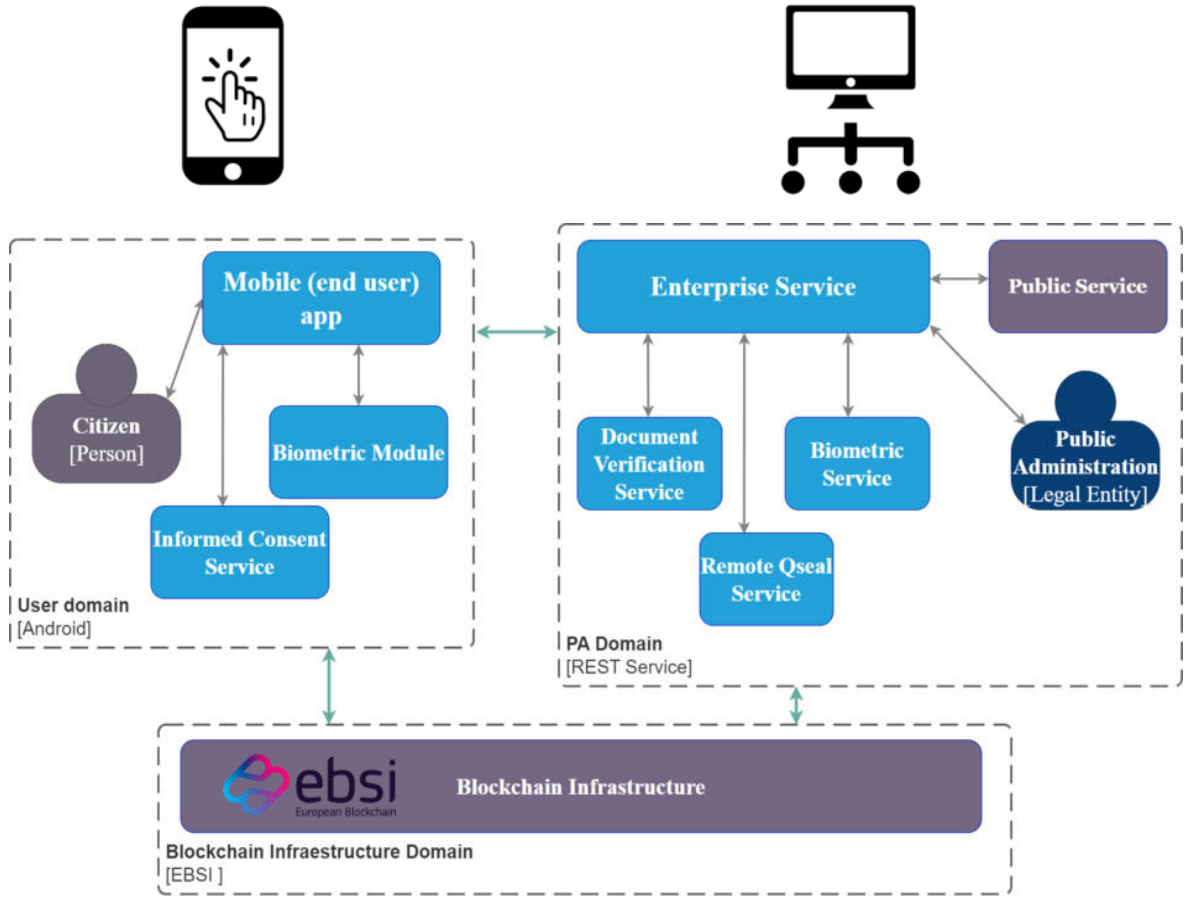


Overview of IMPULSE – Blockchain

La **blockchain** è un registro digitale che tiene traccia di tutte le transazioni effettuate in modo sicuro e trasparente.

Ogni transazione è registrata come un blocco di informazioni, che viene poi aggiunto in modo permanente alla catena di blocchi precedenti. In questo modo, **la blockchain è una sorta di libro mastro digitale** che consente di registrare in modo affidabile e immutabile tutte le attività che si svolgono sulla rete.

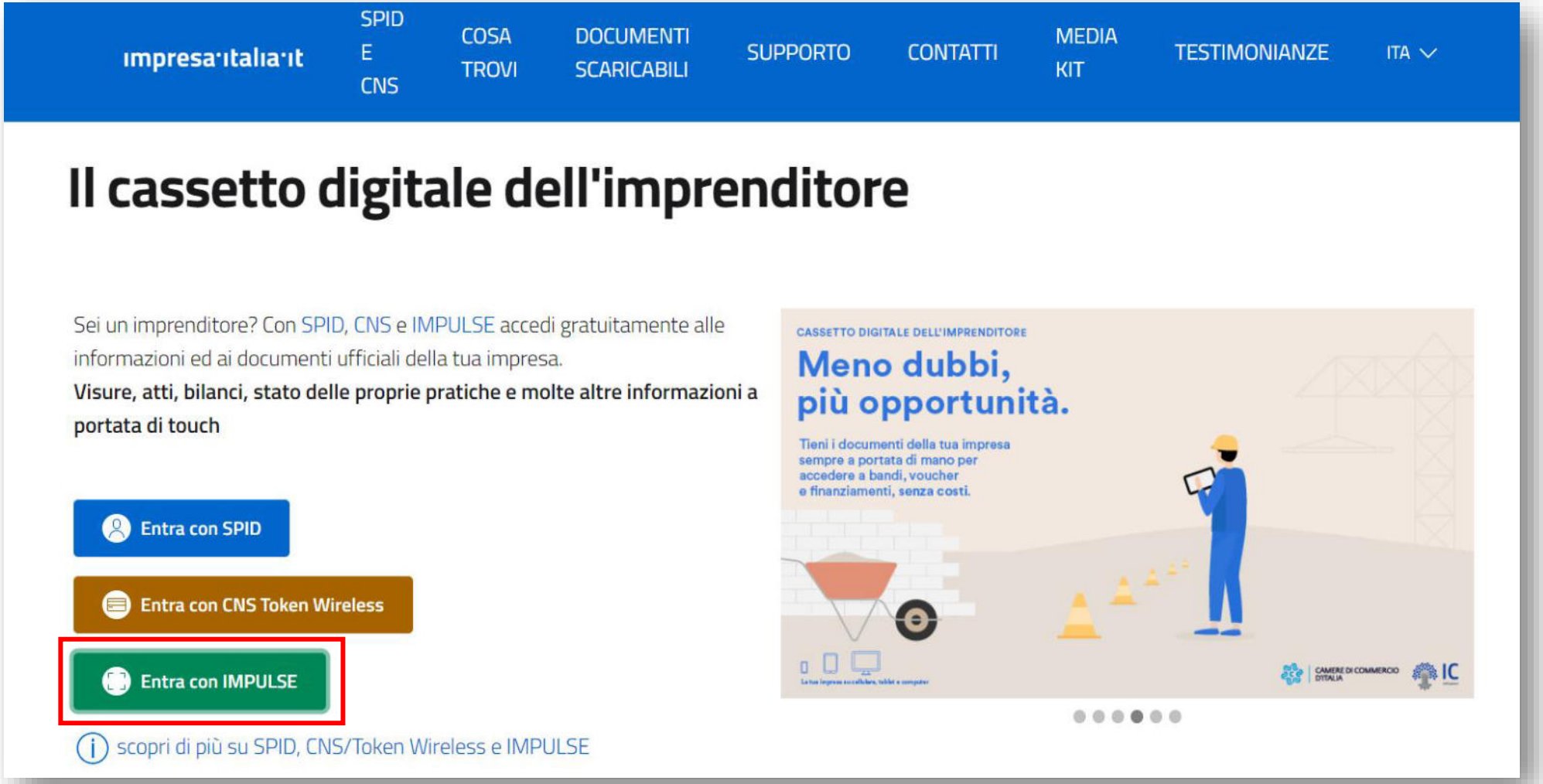
EBSI, o European Blockchain Service Infrastructure, è **una blockchain pubblica, utilizza una rete di nodi distribuiti in tutta Europa,** ed è stata creata dall'Unione Europea per aiutare i governi e le imprese a condividere informazioni in modo sicuro, affidabile ed immutabile.



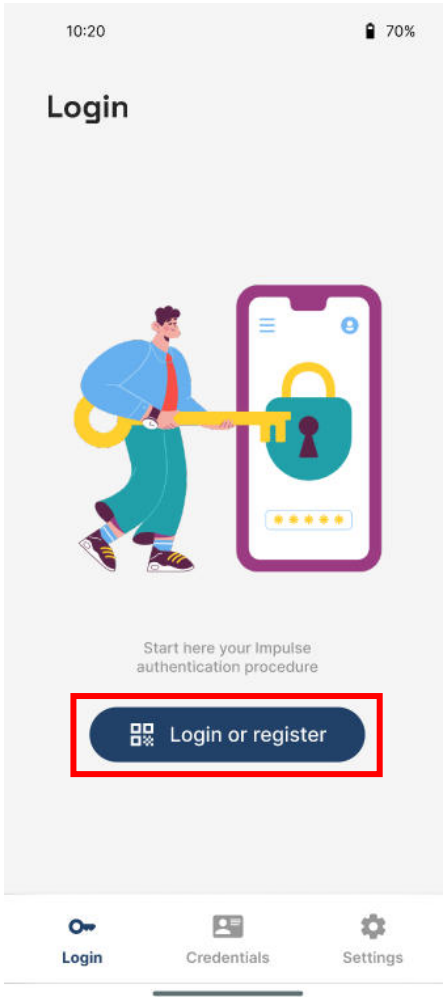
Overview of IMPULSE – SPID vs IMPULSE

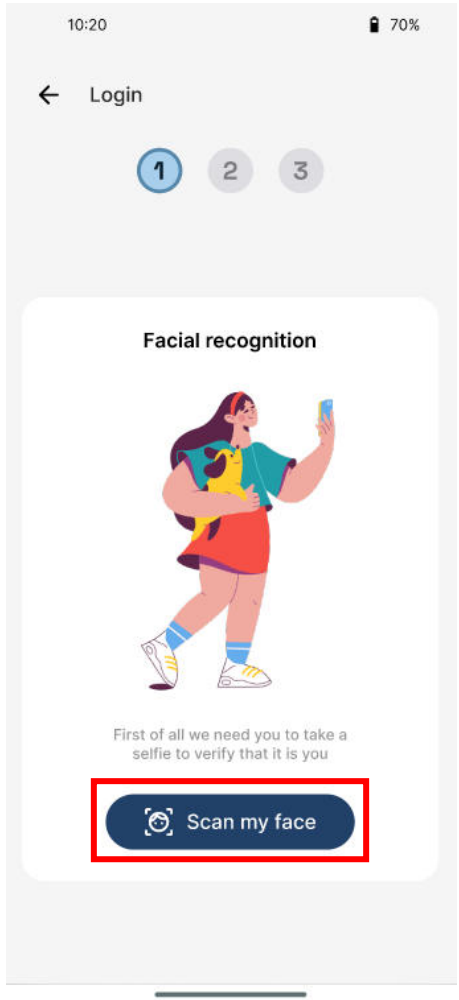
- La **procedura di registrazione** (onboarding) potenzialmente elimina l'intervento umano per verificare l'identità dell'individuo
- **L'integrità dei dati** è protetta dall'infrastruttura europea EBSI basata su tecnologia blockchain
- **L'autenticazione semplificata** non prevede l'uso di password ma solo del riconoscimento del volto
- A tendere IMPULSE avrà la possibilità di **gestire più credenziali** legate alle caratteristiche di un'azienda o di una persona (legale rappresentante d'impresa, titolo di studio, certificazioni d'impresa, certificazione di maggiore età, etc)

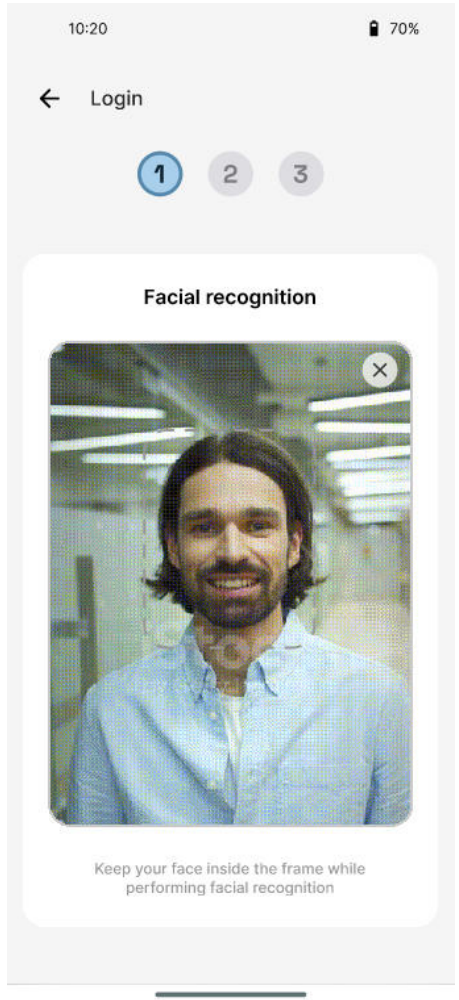
Esempio - Accesso al cassetto digitale dell'imprenditore

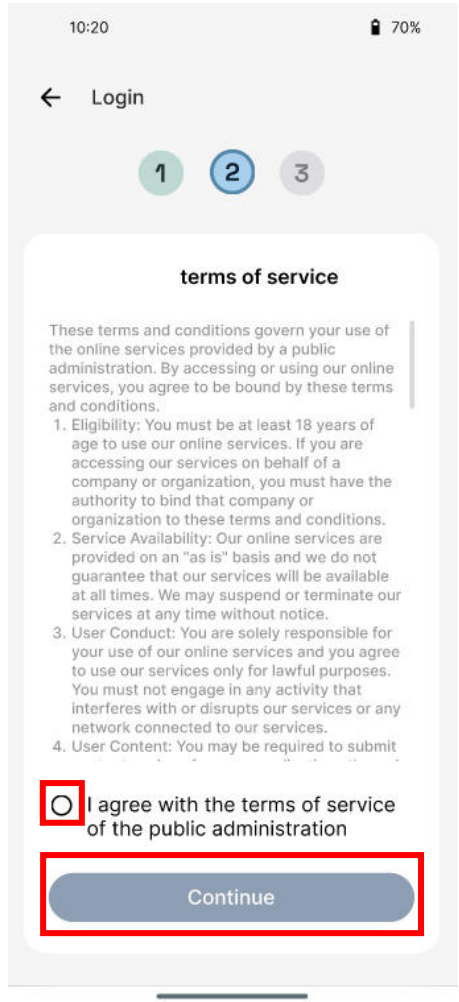


Esempio - Accesso al cassetto digitale dell'imprenditore

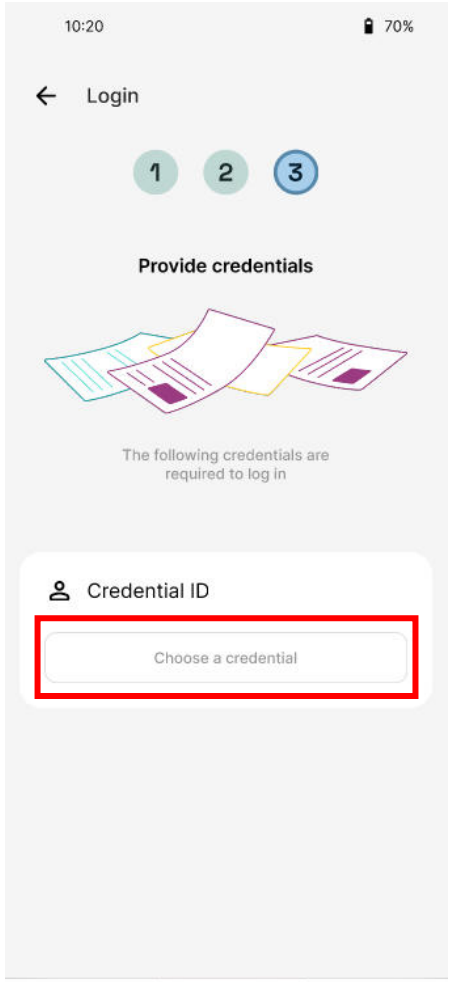


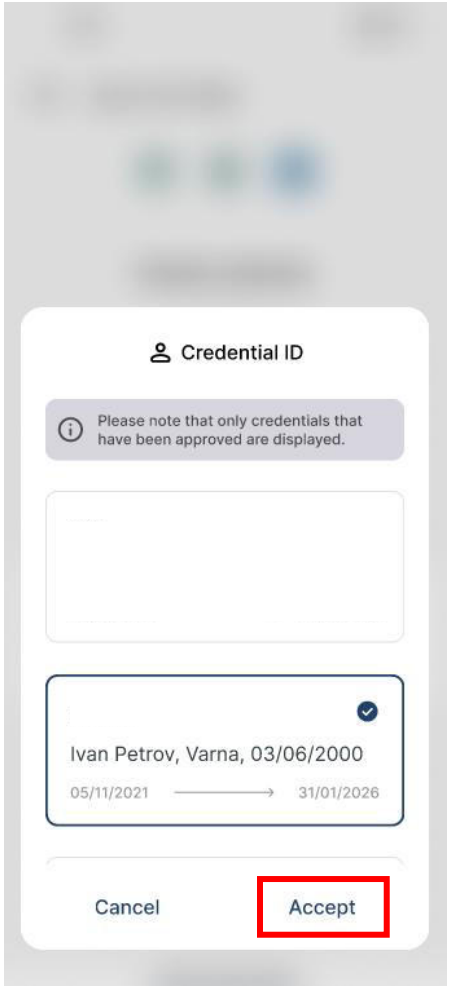


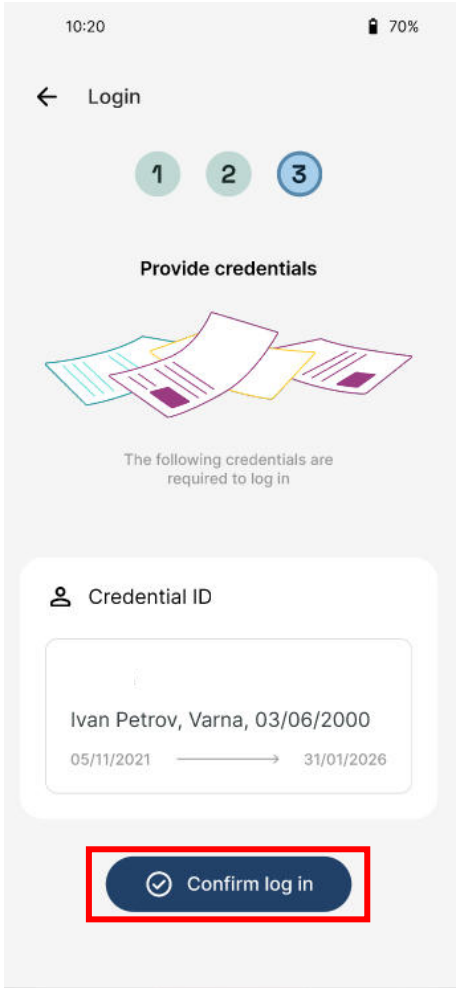


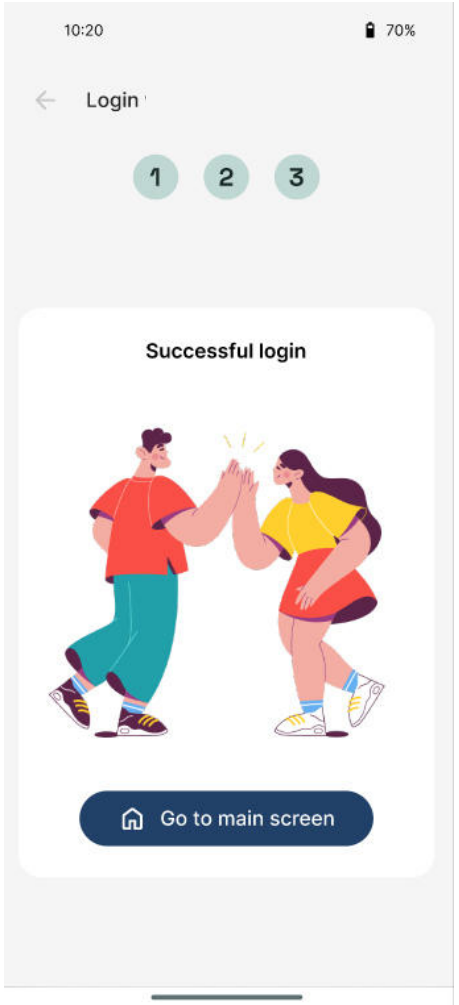


Esempio - Accesso al cassetto digitale dell'imprenditore

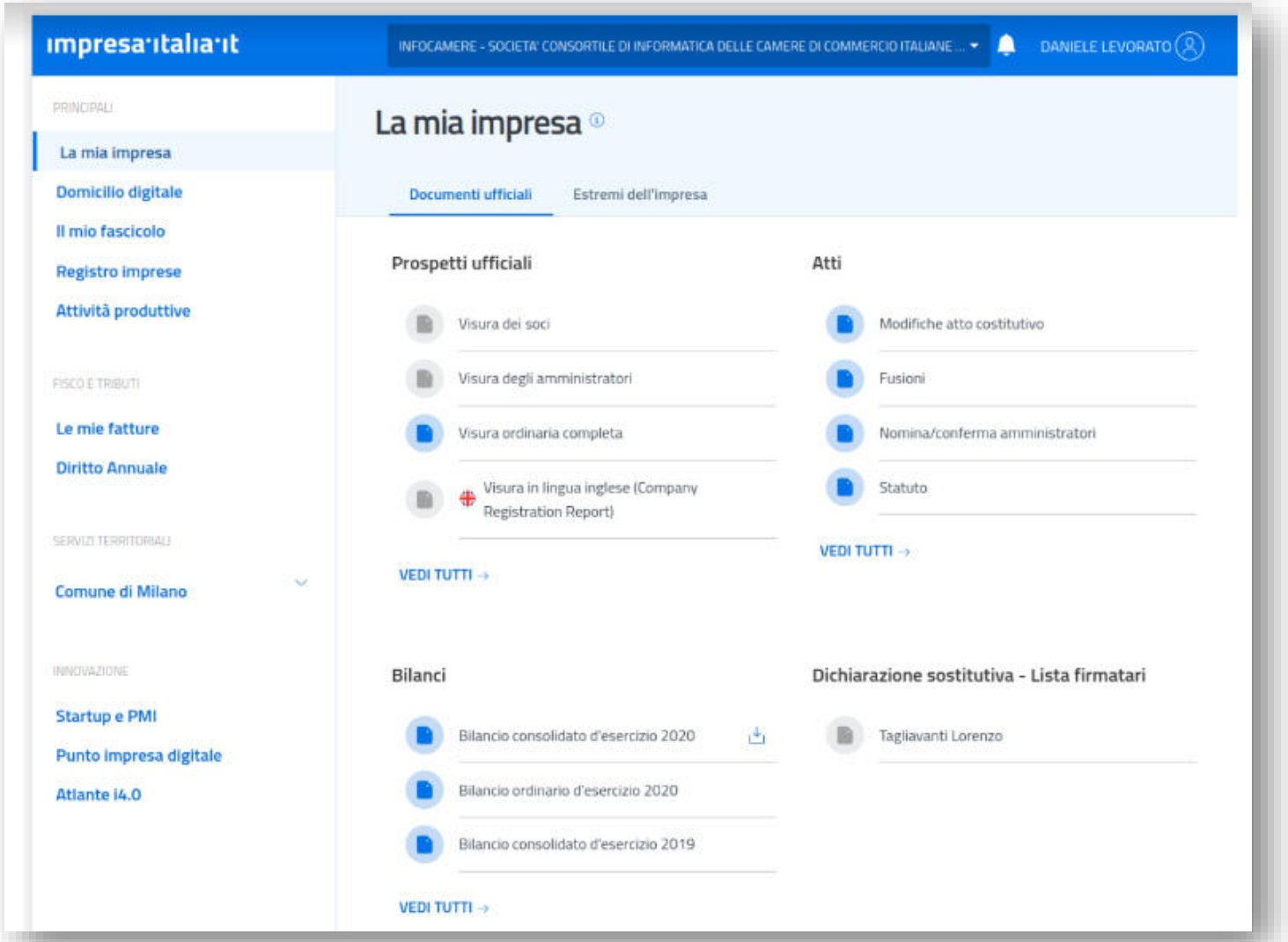








Esempio - Accesso al cassetto digitale dell'imprenditore



Use Cases

- **Dove può essere utilizzata l'identità digitale? (Settore pubblico, privato, ecc)**
- **Quali sfide/difficoltà comporta l'adozione dell'identità digitale in Italia?**
- **Quali sono i timori e i dubbi principali nell'adottare l'identità digitale? (privacy, dati, ecc)**

Impulse

Identity Management in PUbLic SErvices

Online Workshop

Smartphone-basierte digitale Identitäten mit Gesichtserkennung für öffentliche Dienste

Die IMPULSE Lösung, Use Cases, Anforderungen

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

Impulse

Agenda

1. **Begrüßung und Vorstellung des IMPULSE-Teams**
2. **Überblick IMPULSE: Projekt, Technologie und Use Cases**
3. **Q & A**
4. **Break-out Sessions: Möglichkeiten und Hindernisse für die Einführung von SSI Lösungen wie IMPULSE in Deutschland**

Audio-/Videoaufzeichnung:

Wir bitten um Ihre Erlaubnis, den Workshop aufzeichnen zu können
... aber Sie können natürlich auch ablehnen!

Nur Mitglieder des IMPULSE-Teams haben Zugang zu den Aufzeichnungen.

Aufzeichnungen werden nur für Forschung und Projektdokumentation verwendet.

Alle Aufzeichnungen werden spätestens nach Projektende (Januar 2024) gelöscht.

Impulse

Agenda

1. **Begrüßung und Vorstellung des IMPULSE-Teams**
2. **Überblick IMPULSE: Projekt, Technologie und Use Cases**
3. **Q & A**
4. **Break-out Sessions: Möglichkeiten und Hindernisse für die Einführung von SSI Lösungen wie IMPULSE in Deutschland**

Impulse

Agenda

1. Begrüßung und Vorstellung des IMPULSE-Teams
2. **Überblick IMPULSE: Projekt, Technologie und Use Cases**
3. Q & A
4. Break-out Sessions: Möglichkeiten und Hindernisse für die Einführung von SSI Lösungen wie IMPULSE in Deutschland

Impulse

Identity **M**anagement in **PU**blic **SE**rvices

Projektvorstellung

Impulse

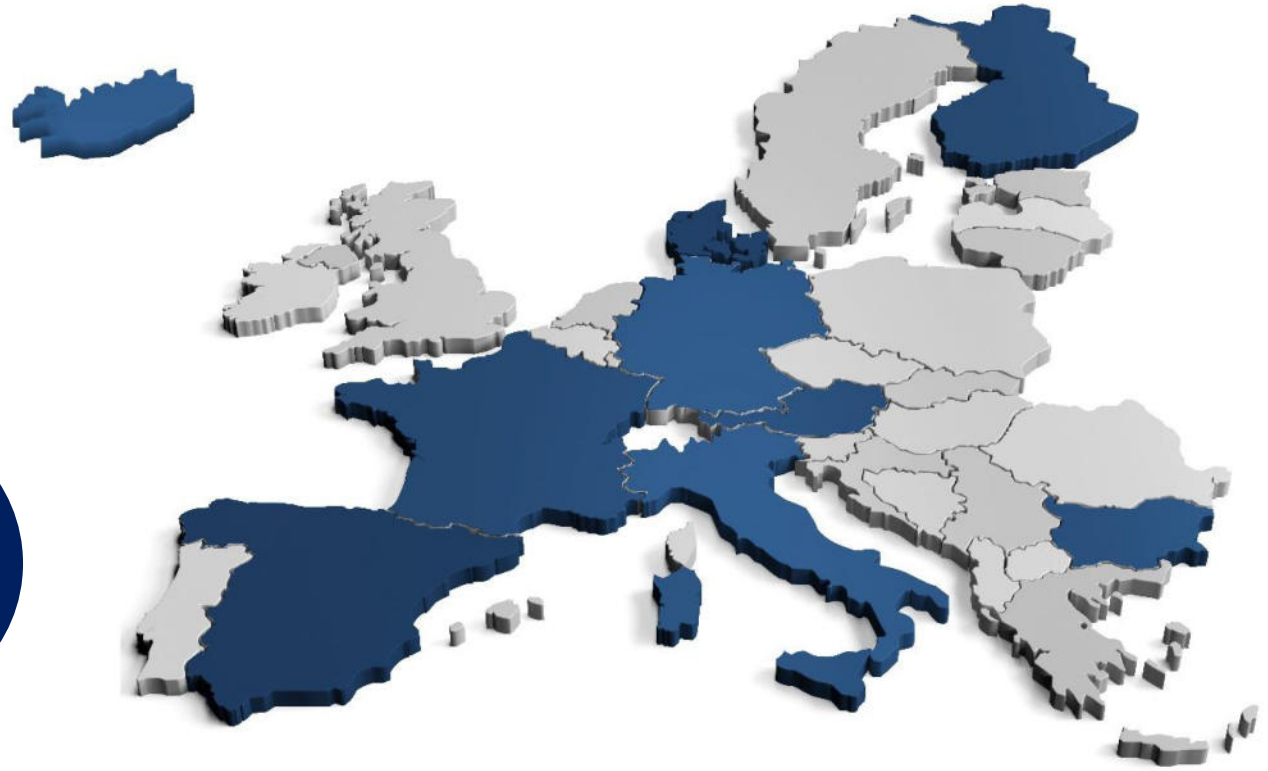
Wer wir sind

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

2021
2024

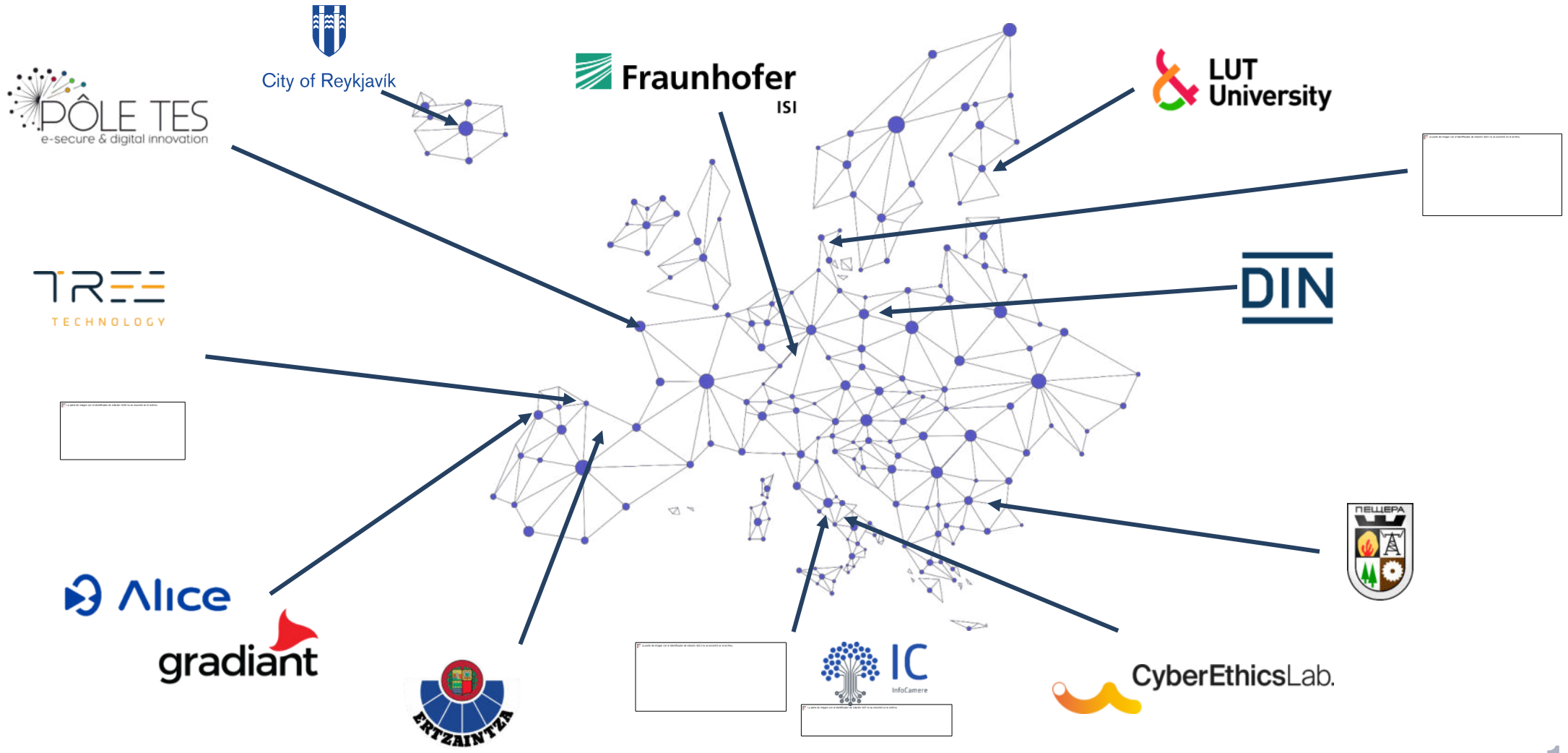
15
Partner

+3M€



Impulse

Die Verbundpartner



Impulse

Projektziele

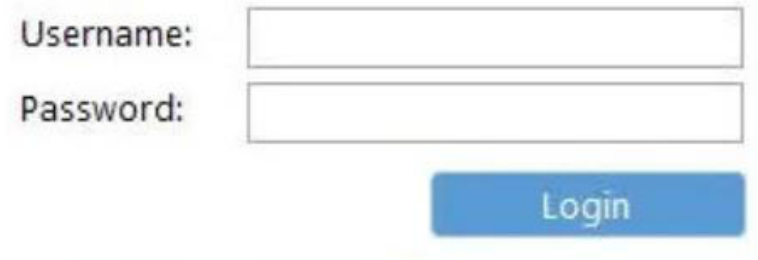
- Entwicklung einer **dezentralisierten, selbstbestimmten digitalen Identitätslösung**, die **Gesichtserkennung** zur Authentifizierung der Nutzer verwendet
- **Erprobung** in **6 Use Cases** in der **öffentlichen Verwaltung** in verschiendenen Ländern
- **Impact Assessment**, Unterstützung von **Regulierung** und **Standardisierung**
- Erarbeitung von **Roadmaps** für mögliche künftige **reale Einsätze** des Systems
- **Ziel bis Projektende**: **TRL 6** (funktionierender Prototyp in Einsatzumgebungen)
- **Optionen nach Projektend**:
  - **Weiterentwicklung** zu **TRL 9** (Kommerzialisierung)
  - **Verwertung einzelner Komponenten** in neuen Lösungen, ev. mit neuen Partnern

Überblick – Elektronische Identitätssysteme

- Herkömmliche eID-Managementsysteme haben zentralisierte Architekturen

User ID und Passwort

- Zentralisierte Identifier
- Datenlecks
- Viele Passwörter



Identity Providers (IdPs)

- Nur ein Passwort, aber...
- Identitäten werden vom IdP kontrolliert
- IdP kann Nutzerverhalten tracken

User Certificates (PKI)

- Schwachstellen bei der Datensicherheit
- Aufwendiger Installationsprozess für „Normalverbraucher“
- Zentralisierte root of trust

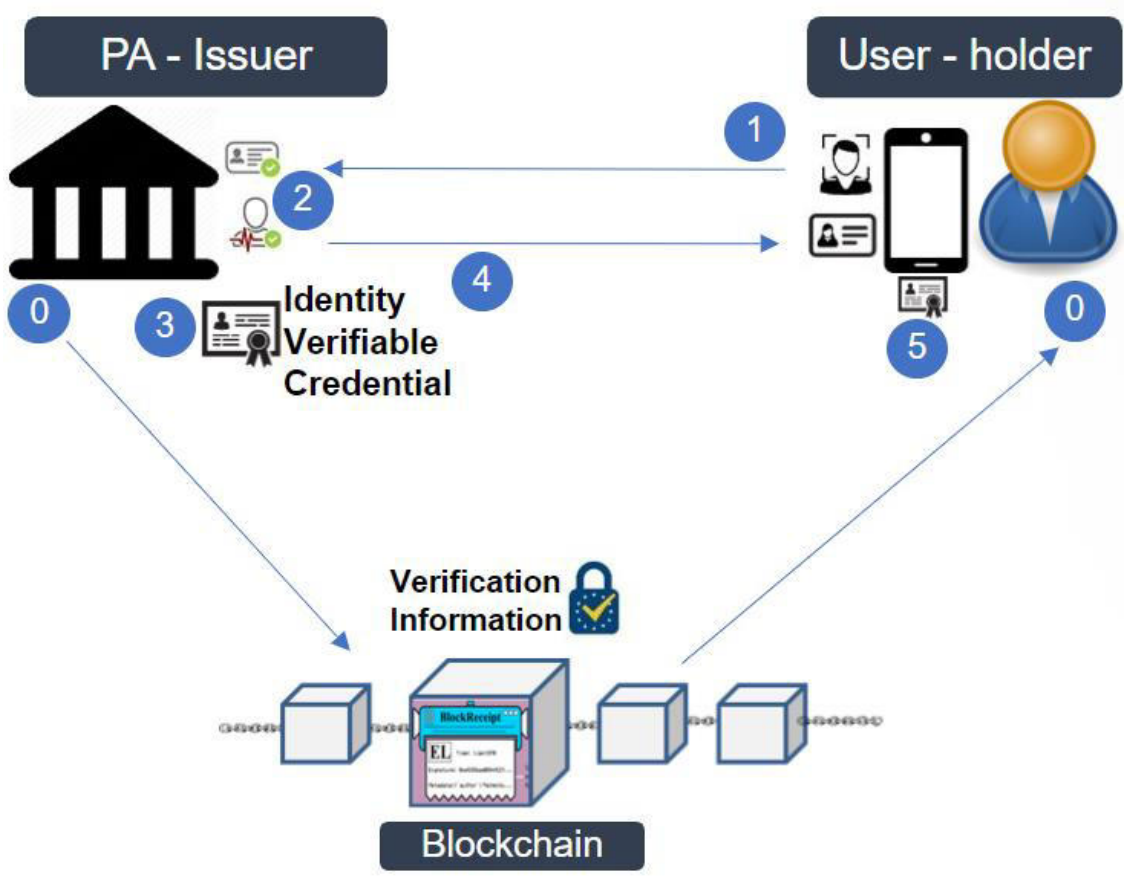
Überblick – IMPULSE als alternatives eID-System

- **Gesichtserkennung** statt Passwörtern – höhere **Sicherheit, Usability, Inklusivität**
- **Dezentralisierte Architektur** – **keine zentrale Instanz** verfügt über die digitale Identität der Nutzer
- **Selbstbestimmt (SSI)** – Nutzerdaten bleiben unter der Kontrolle der Nutzer
- **Technische Umsetzung** mittels sog. **„Verifiable Credentials“,** cryptographisch gesicherte, verifizierbare Identitätszertifikate

Zwei wesentliche Schritte aus Sicht der Nutzer:

- **Registrierung**: Nutzer registriert sich beim Dienste-Anbieter und fordert von ihm ein digitales Identitätszertifikat (Verifiable Credential, VC) an
- **Authentifizierung** („Einloggen“): Nutzer authentifiziert sich beim Diensteanbieter mit dem VC

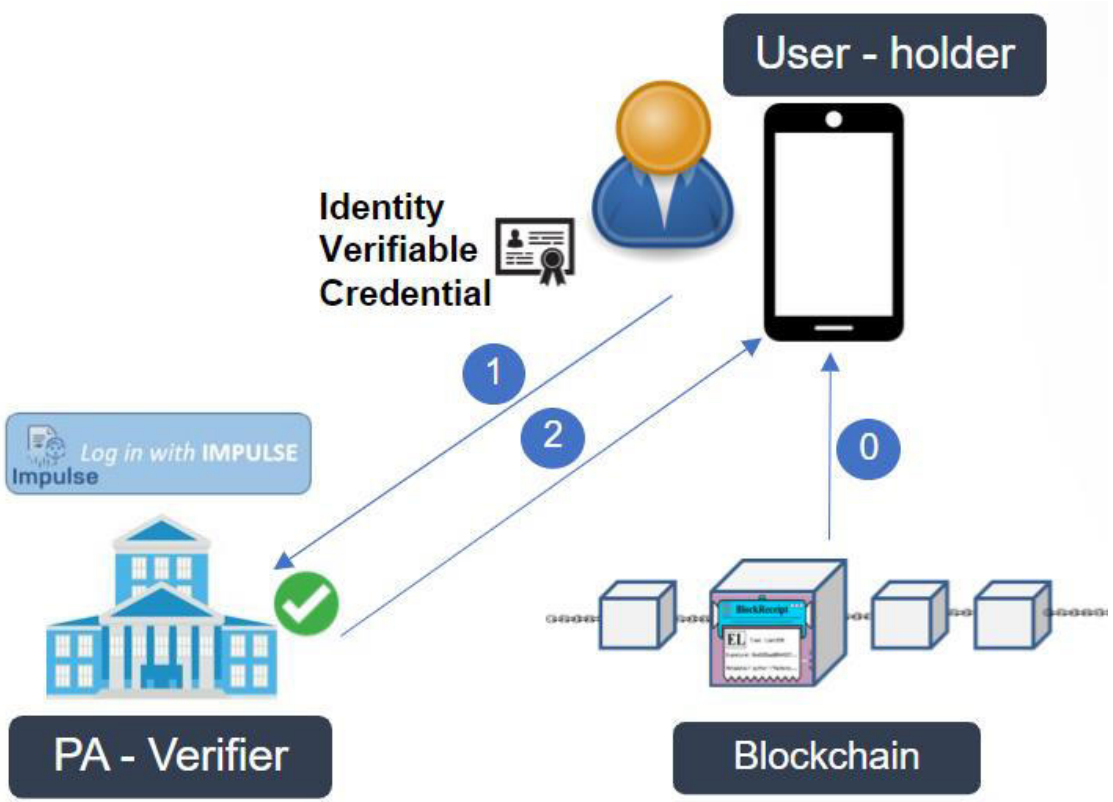
Überblick – Benutzerregistrierung



0. Verification information des Diensteanbieters (PA) (Decentralised Identifier, Public Key, Trusted Issuer Information) wird auf Blockchain gespeichert und vom Nutzer abgerufen

1. Nutzer macht ein Selfie (Kurzvideo) und Fotos seines Personalausweis o. Reisepass
2. Mittels KI prüft IMPULSE
   - Korrelation zw. Selfie und Ausweisfoto
   - Echtheit des Ausweises
   - Extrahiert Ausweisdaten (Name, etc.)
3. Dienstanbieter stellt Nutzer ein „Identity Verifiable Credential" (VC) aus
4. [5.] VC wird auf Nutzer-Endgerät gespeichert

Überblick – Benutzerauthentifizierung



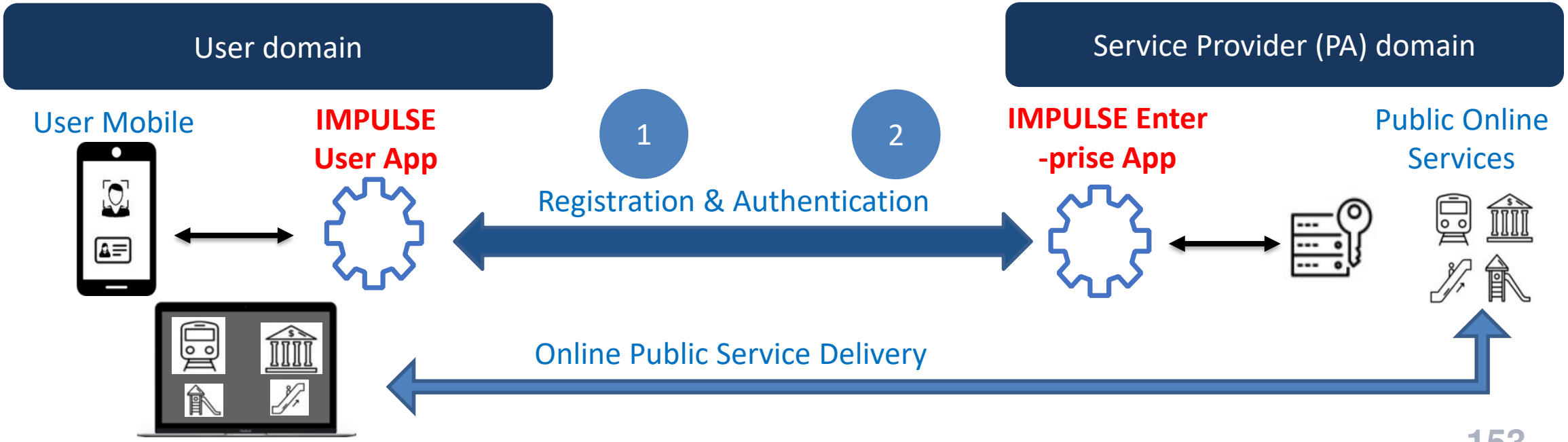
[0] Benutzer ruft die Webseite des Diensteanbieters (PA) auf und wählt “Log in with IMPULSE”

[0] IMPULSE App öffnet sich und ruft die „Verification Infomation“ des Anbieters von der Blockchain ab

1. Nutzer macht ein Selfie, um sich beim Anbieter zu authentifizieren;
2. IMPULSE App zeigt dem Anbieter das auf dem Endgerät gespeicherte „Verifiable Credential“
3. Der Anbieter verifiziert das „Verifiable Credential“ und liefert dem Nutzer den angeforderten Dienst

Überblick – Systemintegration

- IMPULSE kann in jeden Online-Dienst integriert werden
- → Nutzer installiert die IMPULSE Android App (Google PlayStore), Diensteanbieter installiert den IMPULSE Container
- IMPULSE nutzt das EBSI/ESSIF-Ökosystem und EBSI Verifiable Credential Schema



Überblick – kommende Erweiterungen

- **Trusted Execution Environments:** für die Digitale Brieftasche (Digital Wallet) in der Endnutzer-App und für die Enterprise Application beim Diensteanbieter
- **Remote QSeal-Service:** Qualifizierte elektronische Signatur
- **Informed Consent Service:** Smart Contracts zum Management Nutzer-Einwilligungen

IMPULSE Projekt: 6 Pilotanwendungen

Impulse

City of Reykjavík

Reykjavik, Iceland
Better Reykjavik participatory democracy portal

Aarhus, Denmark
Electronic access to personal information and services

Gijón, Spain
Public services app

Unioncamere & InfoCamere, Italy
Enterprise digital drawer

Ertaintza, Spain
Issuing complaints entirely online

Peshtera, Bulgaria
Civil registration & certification

Peshtera, Bulgarien: Geringe Nutzung Digitaler Verwaltungsdienste

Status Quo

- Plattform mit >70 Verwaltungsdiensten existiert
- ...wird aber wenig genutzt: Bürger präferieren F2F Prozesse

→ Kostet Beamte und Bürger viel Zeit

- Ursache: Hoher Aufwand um eine digitale Identität zu bekommen

Lösung durch IMPULSE

- (Viel) einfachere & unaufwendigere Registrierung für Digitale Identität
- Einfache Authentifzierung

→ Spart Beamten und Bürgern Zeit

Ertzaintza, Spanien: Kriminalanzeigen Online

Status Quo

- Kriminalanzeigen (leichte Kriminalität) können bereits Online eingegeben werden
- ... aber Bürger müssen innerhalb von 72 Stunden persönlich vorsprechen und die Anzeige unterzeichnen

→ Kostet Beamte und Bürger Zeit

→ Geringe Nutzung der Digitalen Option

Lösung durch IMPULSE

- Identität kann Online bestätigt werden
- Notwendigkeit, persönlich zu unterzeichnen, entfällt

→ Spart Beamten und Bürgern Zeit

Aarhus: Sichere Dokumentaufbewahrung für Obdachlose

Impulse

Status Quo

- Obdachlosen fehlt oft Möglichkeit, Dokumente o. Wertgegenstände sicher aufzubewahren
- Schließfächer mit Schlüssel oder PIN nur bedingt hilfreich

→ Dokumente gehen verloren

→ Erschwert Reintegration, Zugang zu staatlichen Leistungen

→ Zusatzarbeit für die Sozialdienste

Lösung

- Schließfächer nutzen IMPULSE
- Authentifizierung über Gesichtserkennung

→ Sichere Aufbewahrung

→ Leicht zugänglich

→ Keine Schlüssel o. PIN

Weitere Pilotanwendungen

- **Gijon, Spanien:** Registrierung und Authentifizierung in der “Citizens App” mit IMPULSE, Zugang zu diversen städtischen Online-Diensten
- **Reykjavik, Island:** Registrierung und Authentifizierung in städtischen Foren mit IMPULSE (Pilot mit körperlich eingeschränkten Menschen)
- **InfoCamere, Italien:** Registrierung und Authentifizierung im öffentlichen Unternehmensregister

Feedback von den Pilotanwendungen

Erste "Live"-Tests der IMPULSE-App mit Endnutzern vor Ort im Sept.-Okt. 2022

- Grundsätzlich positives Feedback...
  - 65% würden IMPULSE "wahrscheinlich"/"sehr wahrscheinlich" nutzen, 71% würden es weiterempfehlen
  - Keine Passwörter!
  - Schnellerer und vereinfachter Zugang zu Online-Diensten
  - Positive Assoziationen (bequem, zeitsparend, sicher, nützlich usw.)
- ...Aber es braucht noch ein paar Verbesserungen
  - Manchen war der Registrierungssprozess nicht klar und einfach genug
  - Benachrichtigungen in der App können noch verbessert werden
- Feedback wird jetzt eingearbeitet

Impulse

Agenda

1. Begrüßung und Vorstellung des IMPULSE-Teams
2. Überblick IMPULSE: Projekt, Technologie und Use Cases
3. **Q & A**
4. Break-out Sessions: Möglichkeiten und Beschränkungen der Einführung von IMPULSE in Deutschland

Questions & Answers

Impulse

Agenda

1. **Begrüßung und Vorstellung des IMPULSE-Teams**
2. **Überblick IMPULSE: Projekt, Technologie und Use Cases**
3. **Q & A**
4. **Break-out Sessions: Möglichkeiten und Beschränkungen der Einführung von IMPULSE in Deutschland**
   - Use Cases
   - Technische Aspekte
   - Regulierung und Standards

Impulse

Diskussion

Optionen für IMPULSE in Deutschland

Vorteile und Use Cases

Aus Ihrer Sicht...

- **Welche Mehrwerte könnten Lösungen wie IMPULSE, die SSI und Biometrie verbinden, für Diensteanbieter und Endnutzer in Deutschland stiften?**
- **Welche Use Cases wären in Deutschland vor allem interessant?**
- **Was sind die wichtigsten Anforderungen, die Diensteanbieter und Endnutzer an Lösungen wie IMPULSE (bzw. SSI Lösungen allg.) stellen?**
- **Was wären die größten Herausforderungen bei der Einführung von IMPULSE/SSI Lösungen in Deutschland?**

- **In Kommunen?**
- **Im Bund und den Ländern?**
- **Im der Wirtschaft?**

Technische Aspekte

Aus Ihrer Sicht...

- Welche technischen Anforderungen müssten erfüllt sein, damit die IMPULSE-Lösung im deutschen eID-Kontext eingesetzt werden kann?
- Wie könnte eine Kombination von IMPULSE mit der AusweisApp_2 oder der BundID aussehen? Welche Interoperabilitätsanforderungen gibt es?
- Generell: Wie kann man die Nutzung von eIDs in Deutschland erhöhen?
  - Indem man die **Authentifizierung per Gesichtserkennung** nutzerfreundlicher macht (statt per Brief, PIN, TAN, Karte usw.)?
  - Indem man für den **Loginprozess eine smarte eID/ digital Wallet** nutzt (statt Karte und PIN)?
  - Durch die Einführung von **Self-Souvereign Identity (SSI)-Lösungen**? Sind diese noch notwendig nach der Einführung von BundID?

- **Im öffentlichen Sektor?**
- **In der Wirtschaft?**

Recht, Regulierung und Politik

Aus Ihrer Sicht...

- **Was sind die wichtigsten rechtlichen und regulatorischen Anforderungen, die eine digitale Identitätslösung wie IMPULSE erfüllen muss, einschließlich Zertifizierungen?**
- **Welche dieser Anforderungen sind in der Regel am schwersten zu erfüllen?**
- **Kann eine biometrisch basierte digitale Identität wie IMPULSE als qualifizierte elektronische Signatur verwendet werden?**
- **Was kann die Europäische Kommission tun, um die Verbreitung von digitalen Identitätslösungen in Deutschland zu unterstützen?**

Impulse

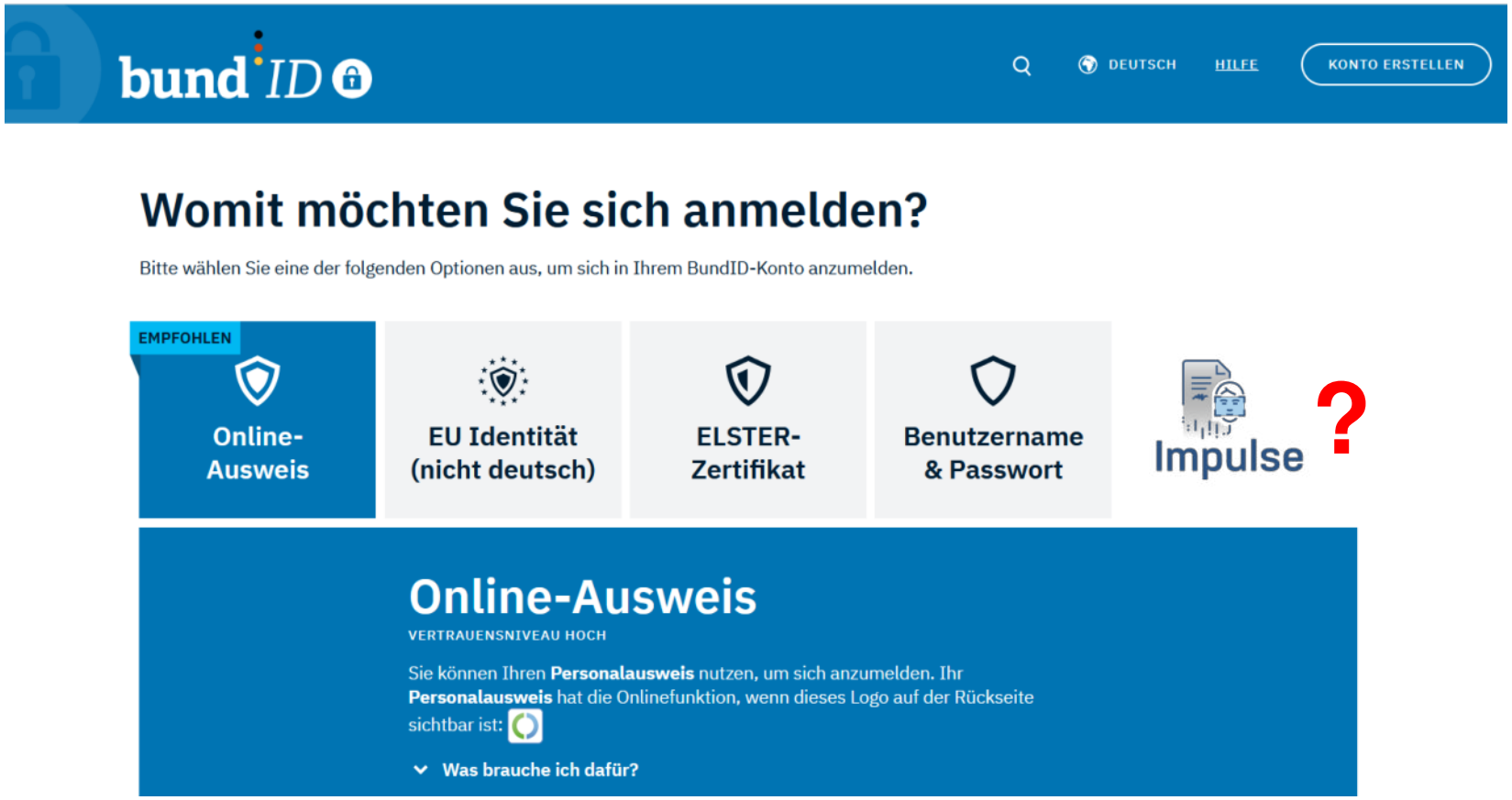
Law, Regulation and Policy

In your view...

- **What are the main legal and regulatory requirements that a digital identity solution like IMPULSE must meet in Germany, including certifications?**
- **Which of these requirements tend to be hardest to meet?**
- **Can a biometrically-based digital identity like IMPULSE be used as a Qualified Electronic Signature?**
- **What can the European Commission do to support the diffusion of digital identity solutions in Germany?**

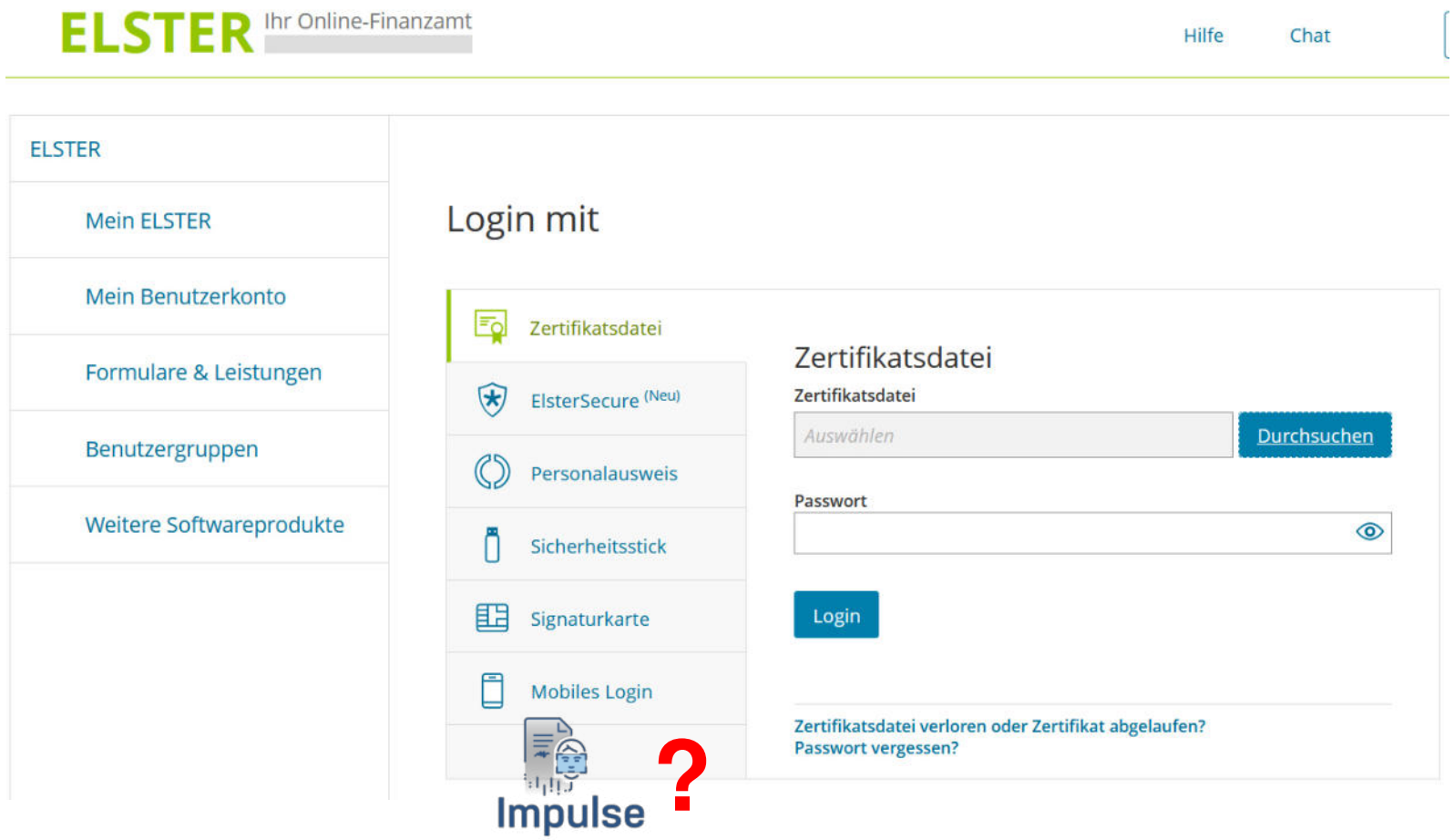
Gruppe: Technische Aspekte

Beispiel: https://id.bund.de



Gruppe: Technische Aspekte

Beispiel: www.elster.de



Die nächsten Schritte im IMPULSE-Projekt

- Zweite Pilotierung des IMPULSE-Systems
- Abschluss des Impact Assessments
- Entwicklung länderspezifischer Roadmaps

Identity Management in PUbLic SErvices

Vielen Dank!

Nicholas Martin nicholas.martin@isi.fraunhofer.de

Bernd Beckert bernd.beckert@isi.Fraunhofer.de

Madlen Schmudde madlen.schmudde@din.de

Xavier Martinez xmartinez@gradiant.org

Iria Nunez inunez@alicebiometrics.com

Luca Mattei l.mattei@cyberethicslab.com

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