D1.2 Updated Member State eGovernment Baseline

Document Identification			
Status	Final	**Due Date**	30/09/2022
Version	1.0	**Submission Date**	03/10/2022

Related WP	WP1	**Document Reference**	D1.2
Related Deliverable(s)	D1.4, D1.6, D1.8	**Dissemination Level (*)**	PU
Lead Participant	JSI	**Lead Author**	Tanja Pavleska (JSI)
Contributors	Tanja Pavleska (JSI)	**Reviewers**	Fredrik Lindén (SU)
			Bob van Os (ICTU)

Keywords :
eGovernment, Single Digital Gateway, eIDAS, Building Blocks, OOP, Digital Service Infrastructures

Document Information

List of Contributors	
Name	Partner
Tanja Pavleska	JSI

Document History			
Version	Date	Change editors	Changes
0.1	20/08/2022	Tanja Pavleska (JSI)	Inserted literature and theoretical background
0.2	23/08/2022	Tanja Pavleska (JSI)	Described methodological framework
0.3	27/08/2022	Tanja Pavleska (JSI)	Entered data visualization
0.4	05/09/2022	Tanja Pavleska (JSI)	Data analysis and discussion
0.5	23/09/2022	Tanja Pavleska (JSI)	Document submitted for internal revision
0.6	26/09/2022	Tanja Pavleska (JSI)	Implemented remarks after first internal review
0.7	27/09/2022	Tanja Pavleska (JSI)	Implemented remarks after second internal review
0.8	27/09/2022	Tanja Pavleska (JSI)	Delivered for final submission
0.9	29/09/2022	Julia Wells (Atos)	Quality review for submission
1.0	30/09/2022	Ana Piñuela (Atos)	Sign off for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Tanja Pavleska (JSI)	28/09/2022
Quality manager	Julia Wells (ATOS)	29/09/2022
Project Coordinator	Ana Piñuela Marcos (ATOS)	30/09/2022

Table of Contents

Document Information 2
Table of Contents 3
List of Tables 4
List of Figures 5
List of Acronyms 6
Executive Summary 7
1 Introduction 9
1.1 Purpose of the document 9
1.2 Structure of the document 9
1.3 Theoretical background 9
1.3.1 eIDAS 11
1.3.2 Digital Service Infrastructures 12
1.3.3 Single Digital Gateway 13
2 Approach and methodology 14
2.1 Approach and objectives 14
2.2 Scope 14
2.3 Data collection and analysis 15
3 eGovernment baseline 18
3.1 eIDAS and the revised eIDAS 18
3.1.1 eID schemes 18
3.1.2 eIDAS-Node 23
3.1.3 Trust services 24
3.1.4 Digital Identity Wallets 26
3.2 Digital Service Infrastructures 28
3.2.1 Blockchain-based solutions 32
3.3 Single Digital Gateway: Life events 33
3.3.1 Digital-by-default 39
4 Discussion 42
5 Conclusions 44
References 45
Annex – Digital Europe for All (DE4A) survey 47

List of Tables

Table 1: Implementation of Digital Service Infrastructures across countries *28*
Table 2: Reuse of building blocks in DE4A *31*

List of Figures

Figure 1: a) Notification status of national eID-schemes b) Level of assurance of eID-schemes 19
Figure 2: Cross-border use of the eID schemes 19
Figure 3: Operating entities of national eID-schemes 20
Figure 4: Implementation of access to services depending on the operating entity 21
Figure 5: Adoption rate of national eID-schemes depending on the operating entity 22
Figure 6: Implementation status of eIDAS-Node 23
Figure 7: Principle of using / enabling foreign eIDs 23
Figure 8: Implementation of trust services 24
Figure 9: Existing monitoring mechanism on the progress of eIDAS implementation 25
Figure 10: Purpose of monitoring mechanisms 25
Figure 11: Existing National Digital Identity Wallets 27
Figure 12: Stage/form of implementation of the solution 27
Figure 13: Validation mechanisms for the Digital Identity Wallets provided by the State 27
Figure 14: Reuse matrix of CEF Building Blocks across Digital Service (and Sub-service) Infrastructures 30
Figure 15: Countries' participation in EBSI, H2020, CEF Digital or RRF projects' use cases 32
Figure 16: Countries employing the Internal Market Information System 33
Figure 17: Means of authentication 34
Figure 18: Mobile accessibility 36
Figure 19: Cross-border availability 37
Figure 20: Appliance of data reuse principle 38
Figure 21: Digitalization of SDG procedures 40

List of Acronyms

Abbreviation / acronym	Description
BRIS	Business Registers Interconnection System
CEF	Connecting Europe Facility
DBA	Doing Business Abroad
DE4A	Digital Europe For All
DESI	Digital Economy and Society Index
DSI	Digital Service Infrastructure
Dx.y	Deliverable number y, belonging to WP number x
EC	European Commission
EESSI	Electronic Exchange of Social Security Information
EFTA	European Free Trade Association
eID	Electronic Identification
eIDAS	Electronic IDentification, Authentication and trust Services
EU	European Union
EU DIW	EU Digital Identity Wallet
GDPR	General Data Protection Regulation
LOA	Level of assurance
MA	Moving Abroad
MS	Member State
NIFO	National Interoperability Framework Observatory
ODR	Online Dispute Resolution
OOP	Once-Only Principle
PDND	“Piattaforma Digitale Nazionale Dati” - The National Digital Data Platform
RRF	Recovery and Resilience Facility
SA	Studying Abroad
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation
SSI	Self-Sovereign Identity
WP	Work Package

Executive Summary

The project Digital Europe for All (DE4A) was launched January 2020. It is a result of the collaboration of 23 organizations from 9 countries of the European Union. The project is funded by the EU Horizon 2020 research and innovation Framework Programme and *"is aimed at creating inclusive digital Environment in Europe ensuring the digital market rights of citizens and businesses by building on secure, privacy-preserving and trustworthy realization of fundamental once-only, relevant-only and digital by default principles"*. Establishing a continuity of large scale pilots, the DE4A reinforces the connectivity of national digital endeavors. Building upon existing infrastructures, it attempts to contribute to an overarching eGovernment network for Europe, supporting parallel efforts from the EC and the Member States to realize the Once-Only Principle Technical System in compliance with the Electronic Identification, Authentication and Trust Services (eIDAS), the General Data Protection Regulation (GDPR) and the Single Digital Gateway (SDGR). Furthermore, it aligns its effort with the EU eGovernment Action Plan 2016-2020, the EU Strategic Plan 2020-2024, Europe's Digital Decade agenda, the Berlin and the Tallinn Declarations and the EIF Implementation Strategy.

The purpose of the present deliverable (D1.2) is to provide a current overview and analysis of the eGovernment landscape in Europe. In that sense, it is a continuation of a previous effort to provide an initial view of the European eGovernment services at the beginning of DE4A. The current report focuses on the means for implementation of e-services and cross-border enablers, identifying existing national eGovernment capacities, major barriers and potential drivers, and establishing a general picture on the implementation levels of the current legislative and technological efforts concerning the eGovernment services. To do that, the study revisits the eGovernment landscape in the domains of Electronic Identification, Authentication and Trust services, and European Digital Wallets (eIDAS / eIDAS v2), as well as the state of implementation of Digital Service Infrastructures (DSIs), the Single Digital Gateway (SDG), and the Once-Only Principle (OOP). The major part of the study is based on data derived from an extensive survey (see Annex: DE4A Survey, and Section 2.3 for more details), which was distributed among the EU and the EFTA countries. The data analysis from the study was complemented by semi-structured experts' interviews, additional data sources that complement the survey dataset, as well as a thorough literature review / desk research.

The results demonstrate several key findings:

- The eID schemes – one of the cornerstones of the cross-border functioning of eGovernment systems – have been widely implemented across the EU. The research suggests that 96% of the eID schemes have been (pre-)notified under the eIDAS regulation, and over 83% responding countries confirmed availability of a national eID scheme. The national eIDAS-Nodes, on the other hand, demonstrate asymmetric readiness for cross-border use, being more advanced in terms of receipt of foreign eID-schemes for national use rather than supporting national eIDs abroad. On the contrary, the implementation of trust services has demonstrated rather homogenous spread across the participating countries.
- Trust towards the role of private entities in the provision of access to public services has been on the rise, although differently exhibited by the different countries. The private sector is increasingly seen as public partner in the context of e-service provision, resulting in a higher percent of public-private partnerships (in 67% of the countries), and covering a significant share of the service market. In addition, with the revision of the eIDAS Regulation, the private sector is also directly included in the requirements for the establishment of the common Toolbox for the technical architecture, standards and guidelines for best practices. Finally, as the revised eIDAS has not entered into force yet, the private sector is the leading factor in providing a transitional model for the European Digital Identity Wallet, offering mobile solutions that work towards infrastructural migration for the upcoming changes.

- The DSIs available at EU level have showed different scale of implementation of both domain-specific and domain-independent building blocks, across countries and in a DE4A context. While some DSIs have been widely set on technical implementation in the EU, others were not referenced by the majority of the respondent countries. Notably, most of the respondents denoted their on-going Blockchain projects, aiming to increase connectivity and transparency of the built solutions.
- The 21 life events announced under the SDG regulation have similarly exposed significant differences in terms of possibility for eID-authentication, mobile accessibility, applicability of the OOP and availability for cross-border use. Showing generally high availability of the services for use with mobile devices and online accessible with the eID, it is of no surprise that cross-border use has also been advancing. However, there is still significant space for improvement of the OOP implementation in terms of law and data harmonization.

Together with D1.4 “Member State Once Only and data strategy Baseline” and D1.6 “Baseline EU Building Blocks supporting Once Only and standard data sharing patterns”, the set of updated deliverables serve as both a testament for the DE4A contribution in the development of eGovernment services in the areas of Studying Abroad, Moving Abroad and Doing Business Abroad (cfr. WP4), and as an experience-based list of policy recommendation that may be used to guide future developments in the area.

1 Introduction

1.1 Purpose of the document

The present report is conducted under the DE4A project and constitutes the D1.2 deliverable. The purpose of this study is to provide an update of the state of eGovernment across European countries, focusing on the domains of electronic identification and trust services, Digital Service Infrastructures and the Single Digital Gateway. The study is complemented by the deliverables: D1.4 "Updated Member State Once Only and data strategy Baseline", which elaborates on the advancement level of the OOP in Europe, D1.6 "Updated Baseline EU Building Blocks supporting Once Only and standard data sharing patterns" and D1.8 "Updated legal, technical, cultural and managerial barriers". Elaborating on the existing infrastructure and practices, these reports contain valuable insights in the DE4A contribution in that regard, especially in the contexts addressed by the DE4A pilots. At the same time, it provides "Lessons learned and recommendations" guidelines for the subsequent developments and policy shaping in eGovernment in the digital European future.

1.2 Structure of the document

This document is divided into five main sections:

- Section 1 sets the context and establishes the theoretical basis of the matters of this study;
- Section 2 elaborates on the methodology employed to carry out the study, as well as the data sources used in the analysis;
- Section 3 presents the results of the analysis by topic, supporting them with discussion and recommendations;
- Section 4 summarizes the obtained results and puts them into the wider EU perspective;
- Section 5 gives concluding remarks and pointers to the other reports that complement the current one.

The document additionally includes an Annex – DE4A Survey, providing a view on the entire questionnaire distributed to the Member States' CIOs. The responses to the survey fed the major part of the data analysis of the report.

1.3 Theoretical background

With the advancement of digital technologies and their penetration into the everyday life of citizens, the European Union's involvement into shaping digital policies and practices has also increased. In order to make the digital transformation beneficial for people and businesses, the Commission proclaimed this period as the Europe's "Digital Decade" [1], devoting to strengthen the digital sovereignty and set its own standards, with a clear focus on data, technology, and infrastructure.

Implemented well, eGovernment enables citizens, enterprises and organizations to carry out their interactions with government more easily, more quickly and at lower cost. Electronic identification (eID) is one of the tools to ensure secure access to online services and to carry out electronic transactions in a safer way. Secure electronic identification is an essential aspect of daily life in the digital world. It is used to check email, shop online and even unlock phones. The COVID-19 pandemic highlighted the importance of this further, as governments and private companies decreased physical interactions to the bare minimum. Therefore, the new European eGovernment policy plans and actions include: the European Union's Digital Compass, which is part of the Digital Decade ambition and aims at 100% online provision of key public services by 2030; the ministerial Berlin Declaration on Digital Society and Value-based Digital Government, which was signed by the ministers responsible for digital transformation in the public administration of the European Union Member States ; the European

Commission (proposed) Declaration on Digital Rights and Principles, which empowers Europeans to fully enjoy the opportunities that the digital decade brings, driven by common European values ; and the European Union Recovery and Resilience Facility, which mitigates the economic and social damage of the coronavirus pandemic by allocating more than 26% of the spending in recovery plans on the digital transition.

Ever since the first large scale eGovernment Action Plan 2011-2015, the European digitalization efforts have followed the necessity for political mobilization of the digital transformation and became one of the milestones toward the establishment of a collaborative network of the EU Member States in the area of government digitalization [2]. With the termination of the Action Plan, the Digital Single Market Strategy was adopted, pursuing the objective for establishing seamless cross-border functioning of public administrations and facilitating public services interactions for citizens and businesses. The subsequent eGovernment Action Plan 2016-2020 continued along the same path, having user-centricity as one of its main objectives and setting a strategic mainframe for the subsequent digital initiatives in Europe. The Tallinn Declaration on eGovernment endorsed the undertaken strategy and elaborated on the principles of digital transformation of public administration [3]. Reinforcing the reduction of administrative burden on citizens and businesses, the adopted strategies have taken Once-Only Principle (OOP) as one of the central elements for the development of the Digital Single Market, leading to the adoption of the EU Regulation on Single Digital Gateway (SDGR). The SDGR, in turn, has aimed at creating a single online point of access to information, procedures and assistance services for citizens and businesses within the EU [4].

With the placement of humans at the core of the European digital services, the necessity for properly addressing citizens' rights has increased. Hence, the EC has proposed a declaration on European digital rights and principles, which are shaped around 6 themes: putting people and their rights at the center of the digital transformation; supporting solidarity and inclusion; ensuring freedom of choice online; fostering participation in the digital public space; increasing safety, security and empowerment of individuals; and promoting the sustainability of the digital future. The EU's objective is to ensure that, by 2030, democratic life and public services online are fully accessible for everyone, including persons with disabilities, while providing easy-to-use, efficient and personalized services and tools with high security and privacy standards. Therefore, the European Commission set out a number of targets and milestones for electronic identification in its Communication 2030 Digital Compass: The European Way for the Digital Decade. For example, by 2030, all key public services should be available online, all citizens should have access to electronic medical records, and 80% citizens should use an electronic identification solution.

In line with the above objectives, DG CONNECT has been developing a European cybersecurity strategy communication, that should accompany the review of the Network and Information Systems (NIS) Directive based on an evaluation of the functioning of the Directive. The revision of eIDAS Regulation will improve its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans.

Complying with the above regulations, DE4A consolidates and extends the vision and conclusions of the relevant projects. Commencing with inventory of the current status of existing digital solutions, DE4A reassesses the eGovernment baseline to provide concrete contributions and directions to pursue the realization of the new Europe's Digital Decade plan [5]. With the idea to shape Europe's eGovernment landscape as a human-centric digital space, WP1 has made the effort to keep track and analyze the advancement of the objectives for inclusive digital environment for the EU citizens and businesses. Throughout its activities and the methodological and technical efforts, WP1 has consistently followed the continuity of regulatory frameworks and requirements, such as the Single Digital Gateway Regulation, the EU eGovernment Action Plans, the Tallinn Declaration and the EIF Implementation Strategy, as well as the revised eIDAS and the new Europe's Digital Decade plan. Thus, the results from this report can be positioned among the recommendations and lessons learned for realization of the new digital targets: a digitally skilled population and highly skilled digital

professionals; secure and sustainable digital infrastructures; digital transformation of businesses; and digitalization of public services.

In the following sections of the report, three major components have been analyzed, which are relevant for understanding the EU countries' advancement in eGovernment:

- Electronic Identification, Authentication and Trust services, including the EU Digital Identity Wallets;
- Digital Service Infrastructures; and
- Single Digital Gateway (shading light on the OOP technical system as well).

1.3.1 eIDAS

1.3.1.1 Electronic Identification Schemes

The regulation on Electronic Identification, Authentication and Trust Services (eIDAS) was adopted on 23 July 2014 and has become a milestone for establishment of regulatory environment to enable secure cross-border interactions among the citizens, businesses and public authorities of the EU Member States [6]. Supporting the development of the internal European market, the adopted regulation urges the EU Member States to modify or repeal inconsistent national frameworks, through development of a coherent and predictable legal environment for accessing services online.

The eIDAS regulation is principally composed of two parts: The first component elaborates on the electronic identification (eID) systems of the EU Member States. Outlining legal base for mutual recognition of national eID systems (which entered into force on September 29th, 2018), the eIDAS regulation enables cross-border electronic identification and authentication among different authorities, thereby stimulating further development of a shared digital space. The notified eID schemes as well as the relying parties where they are used are connected to a national eIDAS-Node, allowing mutual recognition of electronic identities in Europe. Interconnected among the EU Member States, the eIDAS-Nodes build up an eIDAS Network, which enables cross-border eID-based authentication.

1.3.1.1 Authentication and Trust Services

The second component of the adopted regulation, which entered into force on July 1st, 2016, establishes a shared internal market for certain Trust Services which are listed in the Regulation – including notably electronic signatures, electronic seals and electronic timestamps. Elaborating on the minimum standards for the trust services and on principles of technological neutrality, the eIDAS regulation improves the reliability of these services, granting them an equivalent legal status as paper-based processes. Postulating a non-discrimination principle for all of these electronic services as a baseline, the regulation furthermore differentiates between several levels of service – electronic service, advanced electronic service and qualified electronic service (the latter allowing the use of a recognizable EU Trust Mark), depending on the type of trust service – with differing levels of legal certainty linked to each level of service.

A set of implementing acts stipulate the implementation process of the eID schemes and trust services on both national and cross-border perspective, establishing the practical and technical modalities for a European connectivity network. Further, under these implementing acts, notified national eID schemes are mapped against specific qualitative criteria to assess their respective levels of assurance, to establish a method for assessing equivalence between notified electronic identities. To promote transparency of the internal market, the European Commission mandated the establishment of trust lists of qualified trust services and created an overview of notified eID schemes that are providing authentication services to citizens and businesses.

National public administrations within the EU differ significantly in terms of the extent to which they have formally laid out their strategic vision for eID. Some have a stand-alone eID strategy describing key objectives and approaches, others have a section of broader digitalization strategy dedicated to

eID, still others just make a short reference to eID in their digitalization strategy, while for the remainder no strategic document referring to eID has been identified [7].

1.3.1.2 European Digital Identity Wallets

Today, about 60% of the EU population in 14 Member States are able to use their national eID cross-border. Only 14% of key public service providers across all Member States allow cross-border authentication with an e-Identity system, for example to prove a person's identity on the internet without the need for a password. The number of successful cross-border authentications per year is very small, though on the increase. Therefore, in 2021, the Commission proposed a Framework for a European Digital Identity [8], which would be available to all EU citizens, residents, and businesses in the EU. It should enable citizens to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phone. They will be able to access online services with their national digital identification, which will be recognized throughout Europe. Under the new Regulation, Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (e.g. driving license, diplomas, bank account).

To make it a reality as soon as possible, the proposal is accompanied by a Recommendation, which requires Member States to establish a common toolbox by September 2022 and to start the necessary preparatory work immediately. This toolbox should include the technical architecture, standards and guidelines for best practices. Clearly, very large platforms will be required to accept the use of European Digital Identity wallets upon request of the user, for example to prove their age. The wallets may be provided by public authorities or by private entities, provided they are recognized by a Member State. The European Digital Identity Wallets will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data, thus having control of the data they share.

In parallel to the legislative process, the Commission has already started working with Member States and the private sector on technical aspects of the European Digital Identity. Through the realization of the European Digital Identity framework, many Member States have foreseen projects for implementation of the e-government solutions, including the European Digital Identity in their national plans under the Recovery and Resilience Facility. The 2030 Digital Compass sets out a number of targets and milestones which the European Digital Identity will help achieve. For example, by 2030, all key public services should be available online, all citizens will have access to electronic medical records; and 80% citizens should use an eID solution.

These activities contribute to address the shortcomings of the (old) eIDAS by improving the effectiveness of the framework and extending its benefits to the private sector and to mobile use.

1.3.2 Digital Service Infrastructures

With a notion on the available set of digital tools, the DE4A constructs upon reusable Digital Service Infrastructures (DSI). Developed under the CEF program, the DSI fulfils the role of a central hub platform, linking up national service infrastructures and via this creating a network of interconnected national infrastructures in Europe.

Encouraging reuse of the existing solutions, the CEF program fosters development of standardized building blocks such as eID, eSignature, and eDelivery, which can be reused in multiple digital services independently from the technological environment and which are relevant to DE4A as common fundamental for cross-border interoperability in the context of the SDG fully online procedures and evidence exchange. Promoting adoption of the available DSIs, the CEF attempts to reduce implementation costs, time-to-market and to improve cross-border technical compatibility. This is to be achieved via the introduction of ready-to-implement solutions replacing some routine and most commonly needed processes (such as electronic identification of users, activation of documents, exchange of messages etc.).

These basic DSIs are complemented with a set of sector-specific DSIs, which are applicable in certain policy areas, such as health or procurement but also in Social Security (EESSI) and Business Registers (BRIS), which are of direct relevance to some of DE4A piloting areas. Developed in compliance with the existing EU legislation, the sector specific DSI are expected to facilitate the alignment of national legislation with the European regulations.

1.3.3 Single Digital Gateway

EU citizens and businesses, especially those operating in another EU country, often struggle to understand the procedures and rules applying to the administrative procedures of interest. Information is often confusing and scattered across different websites, lacking any guarantee of quality or reliability, and leaving their questions unanswered. A number of procedures are still paper-based, requiring queuing in an office and causing waste of time and money. In addition, cross-border users often run into obstacles with national administrative procedures because they only work with national solutions and methods. Citizens and companies are even unaware of the possibility to get assistance services to help them solve their problems. This holds back the realization of the EU vision for a single digital market ensuring the freedom of goods, services, capital, and people. It also hampers the establishment of a digital single market by building unnecessary online barriers between people in different EU countries. To address these problems, the European Parliament and the Council of the European Union adopted a regulation establishing a single digital gateway on 2 October 2018 It is expected to save companies more than €11 billion per year and boost cross-border activity. Access to the gateway is enabled via a search function in the Your Europe portal, which has been providing EU and national information on the rights of citizens and businesses, as well as access to assistance services. The EU Regulation on Single Digital Gateway (SDGR) creates a single online point of access to information, procedures and assistance services for citizens and businesses within the EU [4]. Information imposes obligation onto public administration to provide exhaustive and reliable information for the citizens to attain national or cross-border services. By the end of 2023, Your Europe is envisaged to offer access to all 21 online procedures in all EU countries, with some of the procedures such as registering a car or claiming a pension being fully digitalized and eliminating the need for paperwork. The most important administrative procedures for cross-border users will be fully available online in all EU countries.

The SDG regulation elaborates on the list of 21 essential life events identified as the priority for digitalization. These life events are related to birth, residence, studying, working, moving, retiring, and starting, running and closing a business and they are expected to significantly release administrative burden from the EU citizens. The Regulation stipulates the equality of the online access for both national and cross-border completion of procedures established at national level related to such life events (referred to in point (b) of Article 2(2)), postulating the necessity for online availability of these services in non-discriminatory manner for cross-border users and for eID-enabled authentication. Further, the development of the services is framed by the once-only principle, which should be equally applied for cross-border procedures.

A system to transfer documents needed for these procedures between national authorities in different EU countries will also be included. For example, a diploma obtained in one country can be shared with the national authorities of another, where it is needed to start a business.

To improve policy making, users are also able to provide feedback through the gateway on obstacles they encounter in the single market.

2 Approach and methodology

2.1 Approach and objectives

The approach taken in this study aims to achieve several outcomes: first, it investigates the existing eGovernment landscape in Europe to provide insight into the state of the various digital public services. This is approached both from national and from cross-border aspect. Second, the study brings in both internal and external know-how to analyze the results and to investigate related issues and topics. This is done through semi-structured experts' interviews, and through a thorough desktop research. The internal factor implies connecting with project-relevant sources (architecture, pilots, legal and governance experts), whereas the external factors means relating to complementary initiatives (EBSI/ESSIF, mGov4EU and TOOP) and relevant EC-experts (DG DIGIT, DG GROW, DG CONNECT). Although the initial plan was to use the results of the study for comparative analysis, together with the results from the first phase, this analysis can be limited to a narrow scope due to several reasons: first, the methodology that was followed in the first phase had to be revised and updated, leading to differences in both the survey and the calculation methodology; second, the feedback obtained from the Member States does not provide consistent datasets that can be compared even along the same indicators. Not all MSs from the first phase provided feedback in the second phase, and those that did have not provided consistent answers. Finally, drawing any conclusion on the progress of DE4A based on this data will make no sense, as the state of eGovernment across Europe depends on many ongoing initiatives with simultaneous, yet separate impact. However, such analysis, in a complete and consistent manner are available from other sources [9], [10].

It is also important to note that it is not a study that can be used for deriving compliance levels of the EU Member States with the European regulatory and policy frameworks. Neither the nature of the methodological framework nor the quality of the obtained feedback allows for such rigorous statements. At best, the results from this study can be seen as pointers to existing good practices, risks and challenges, drivers and enablers for the European digital transformation goals. The strength of the study in its methodological framework that can be reused and adopted by other future initiatives aiming to contribute to the continuity of digitalization efforts in EU.

The results are mainly represented in an aggregated format, but they also offer a view into some Member States' peculiarities. Making an inventory of the existing eGovernment practices, the report portrays the overall European advancement of the EU Member States, revealing the most crucial developments and pitfalls of the existing European digital space. Based on the obtained results, the study explores the perception of the participating countries of their digital advancement and suggests a ground for further actions.

2.2 Scope

In the context of the identified objectives, the present study attempts to provide a generalized view on the European eGovernment landscape. To achieve this goal, the conducted research approached the overall topic from several major points relevant for the European digital space:

- *Electronic Identification and Trust Services (eIDAS)*. The research is composed of three major constituents, namely: electronic identification scheme (eID-schemes), eIDAS-Node and trust services, and EU Digital Identity Wallets. The findings, on one hand, comprise the general information on the deployed national eID schemes – including their characteristics, participation in the EU cooperation on the eID notification and their actual use indices – and on the other hand, the current status of the eIDAS-Node cross-border interoperability. The findings are complemented by the review of the implementation level of trust services, elaborated in the eIDAS regulation.
- *European Digital Identity Wallets (EU IDW)*. In view of the latest development on eID and the revision of the eIDAS regulation, this part stand at the intersection between eIDAS and the OOP,

providing information on the potential transition models present across European countries in the form of (mobile) digital identity wallets.

- *Digital Service Infrastructures (DSI)*. The report reflects the major achievements on implementation of Building Block and sector-specific DSIs, elaborated under the Connecting Europe Facility (CEF) and other EU programs.
- *Single Digital Gateway (SDG).* The research aims to take stock at the existing level of implementation of the essential 21 SGD life events (procedures) for citizens and businesses (as listed in the Annex 2 of the SDG Regulation). The implementation level of the SDG life events is performed from the perspectives of the available authentication method, accessibility for mobile devices, compliance with the OOP and availability for cross-border use.
- The geographical scope of the research was covering the 27 Member States of the European Union and was additionally complemented by the EFTA states (Iceland, Liechtenstein, Norway, and Switzerland). The survey questionnaire (see Annex) was sent out to 31 state representatives, covering the aforementioned eGovernment initiatives. The responses were received from 18 countries (17 Member States and 1 EFTA country) - Austria, Belgium, Bulgaria, Croatia, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, Netherlands, Portugal, Romania, Slovenia, Spain, Sweden, Hungary, and the Czech Republic – amounting to a representativeness of 58% of all (EU+EFTA) countries, and 63% of the Member States.
- Measuring the performance of the EU Member States in the context of the cross-border European initiatives, the research likewise attempts to evaluate the advancement of national eGovernment agenda. Conducting an inventory of the availability of certain eGovernment aspects for national usage, the research investigates the availability of local and regional solutions and approaches toward implementation of the Digital Agenda for Europe.

For the second phase of data gathering, several changes were made prior to survey submission:

- First, the survey was revised to lower the amount of subjectivity inserted by the answers in the first phase;
- Second, the topics of interest were revised to match the current EU trends on eGovernance. Thus, the existing survey chapters were revised in terms of redundancy, and an entirely new chapter on Digital Identify Wallets was added.
- Third, the methodology was revised to allow for simpler, yet less subjective data analysis;
- Finally, the overall approach was revised based on the reviewers' comments, the experiences from the first phase of data gathering, and the remarks obtained from internal and external project partners.

It is important to note that the present report should not be seen as an isolated WP1 deliverable, but as piece of a deliverable set whose parts complement each other. Thus, all four deliverables: D1.2, D1.4, D1.6, and D1.8 should be read as a single document.

2.3 Data collection and analysis

Combining both qualitative and quantitative research methods, the study used following data sources for the assessment of the eGovernment baseline:

- *Data collection survey*. The survey was targeted at the current eGovernment advancement of European states and consisted of 5 major subjects: Electronic Identification and Trust Services, European Digital Identity Wallets, Single Digital Gateway, Digital Service Infrastructures and Once-Only Principle and Data Strategy. The online survey was distributed to the Member States' CIOs of

and EFTA countries and the data was collected between March 31st and August 22nd, 2022. The respondents were suggested to also evaluate the performance of their countries with respect to the indicated topics. The questionnaire offered the respondents a possibility to supplement the submitted data with additional comments illustrating country-specific context relevant for understanding the particular eGovernment initiative.

- *Desk research*. The insights derived from the survey are supplemented by the analysis of the existing policies and reports relevant for comprehension of the general eGovernment domain, as well as its advancements along the five topics of interest. The EU policies stipulating development of the shared European digital space have been used as a guideline for survey design and analysis. At the stage of the response analysis, the data obtained via the survey was supported by contextualization of the EU MS' eGovernment development through research of relevant national strategies and legislative frameworks. The results from the survey provide the basis for rich context analysis of the respected country, but more important – for drafting policy recommendations supporting each stakeholder in the process of digital transformation through policy compliance.
- *Semistructured experts interview*. One of the distinguishing traits of this study compared to the more general overview reports (such as the eGovernment Benchmark reports, the Digital Economy and Society Index (DESI) and NIFO (National Interoperability Framework Observatory), is the ability to obtain information at a more granular level. This information comes from several sources: the DE4A pilots, the architecture iterations in relation to the implementation practices within DE4A, the contextual know-how obtained from the shared experiences with related initiatives (TOOP, SEMPER, BRIS, mob4Gov, etc.), and the dedicated experts interviews on the topics of interests. The results from the later are integrated into each of the major themes of the survey, enriching the contextual analysis of the survey results. More importantly, the insights from these interviews allow us to view the results from several different perspectives and address the whole spectrum of eGovernance stakeholders.

During pre-processing, survey data was cleansed and checked for consistency. Moreover, contextual information was extracted from the respondents' comments to add relevance to the analysis and to allow for a more granular view of the discussed issues. If needed, direct communication with the respondents was established to clarify the point of either the question or the position response of interest.

One major point that distinguishes this report from the previous (the one delivered from the first phase of data gathering) is the removing of the calculation methodology. The employment of this methodology was deemed as an inappropriate effort for several reasons: first, the methodology was applied to a data containing too subjective answers, making it both inaccurate and inadequate. Second, it was applied to an incomplete dataset and for the purpose of scoring and ranking, which leads to incorrect results.

- *Meaningfulness of the responses*. For the survey targeted at the member sates' CIOs, it suggested the respondents to complete the questionnaire at best of their knowledge, leaving out the possibility for abstaining from the answer if the information was not available. Unlike in the first phase, when the answers or choices of "Do not know" and "Not applicable" were not included in the quantitative analysis, these answers are included and considered as relevant to be shown in this phase. The reason for this is to get the impression about the respondents' engagement with the respective questions as a form of feedback that can trigger additional methodological revisions.

The results of the study reflect the current advancement of eGovernment of Europe, but it relies to a great extent on the information provided by the CIOs of the European countries. Acknowledging the challenge of gathering multifaceted information on eGovernment performance aggregated at the national level, such an approach influences the impartiality of the study. Furthermore, the fact that the survey achieved a response rate of 58% (63% among the Member States), requires to complement

the analysis with information from additional sources. Moreover, this data should be consistent methodologically in order to provide relevant back up with information. For similar reasons, the study cannot be assumed to be representative for the complete geographical scope as well. These drawbacks have been partially overcome by the exhaustive desk research, the context analysis based on the free-text comments in the survey, as well as the semi-structured experts' interviews. The latter is also an argument towards mitigating the risk of biased representation of survey information.

This report has a few limitations. The main one relates to comparability of the country analysis that results both from the second phase and between the two phases. The reason is mainly the incompleteness of data obtained through the surveys and the low quality of the obtained feedback. In addition, not all countries that provided responses are the same in both phases. However, even if such feedback was perfect in both of the phases, it is not reasonable to draw conclusion about the contributions of DE4A for such outcome, as DE4A is not the only initiative that has been supporting the realization of Europe's eGovernment agenda. Therefore, where available, we support out results with data from other reports as well, but we abstain to make any comparative analysis, as data comes from different sources and is based on different methodologies.

3 eGovernment baseline

In this section, we first provide a high-level view on the specific topics investigate through the survey, and then present the concrete results from the survey data analysis.

3.1 eIDAS and the revised eIDAS

The Electronic Identification, Authentication and Trust Services (eIDAS) Regulation provides the basis for cross-border electronic identification, authentication and website certification within the EU [6]. EU Member States may notify and recognize, on a voluntary basis, national electronic identification schemes in their Member States. The recognition of notified electronic identification became mandatory in 2018. Already 60% of Europeans can benefit from the current system but take up is low, their use is cumbersome and business cases are limited.

So far, there has been no requirement for Member States to develop a national electronic identification and to make it interoperable with those in other Member States. This has led to discrepancies between countries. Therefore, a new proposal for a Regulation on digital identity has been rolled out, which addresses some shortcomings in eIDAS by improving the effectiveness of the framework and extending its benefits to the private sector [11]. It should allow Member States to offer citizens and businesses digital wallets that will be able to link various aspects of their national digital identities. These may be provided by public authorities or the private sector if they are recognized by the Member States. In addition, citizens should also be able to access services online without having to use private platforms or share personal data, having full control of the data they share.

To accelerate the implementation of this idea, the proposal for the updated Regulation has been accompanied by a Recommendation [12], allowing the Member States to establish a common toolbox (by September 2022) and to start the necessary preparations. The scope of the toolbox should cover all aspects of the functionality of the European Digital Identity Wallets and of the qualified trust service for attestation of attributes. It should include the technical architecture, standards and guidelines for best practices in order to allow a smooth transition towards the Regulation once it is approved.

By 2030, the EU framework should lead to wide deployment of a trusted, user-controlled identity, allowing each citizen to control their own online interactions and presence. Users should be enabled to make full use of the online services easily throughout the EU, in a secure and trustworthy manner.

3.1.1 eID schemes

Electronic identification (eID) means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. Based on the joined dataset obtained from our survey and the eID Community wiki [13], 29 European countries, among whom all Member States have at least one eID scheme in place. Of the 29 countries, 23 have at least one eID scheme that is notified under the eIDAS Regulation (Figure 1a)). Five countries (Portugal, Poland, Bulgaria, Hungary and Liechtenstein) do not have a notified eID scheme in place yet are in the process of pre-notification, and one (Norway) has its eID scheme peer-reviewed. Hungary was preparing for pre-notification at the time of providing feedback to our survey, which is why we count it among the countries with pre-notified eID scheme. The Act CCXXII on the general rules of electronic administration and trust services is the reference document guiding the transposition of the eIDAS within the national law. Almost all 29 countries have at least one eID scheme with High level of assurance (LoA), except Denmark and France, whose eID schemes have Substantial LoA (Figure 1b)). However, activities across all countries are moving towards meeting the requirement for a notified eID scheme as part of the revised Regulation. For example, the project “Centralized Software Platform for Digital Identification - PSCID” in Romania has as general objective the improvement and automation of the access to government electronic services for citizens, and ensuring the unique electronic identity of each citizen using eGovernment electronic services. A part of the project activities, it is envisaged

to establish the National Electronic Register of Electronic Identities, which will integrate the electronic identities of all users of eGovernment electronic services. At this point, the specifications and the configuration of the test/development/production environments are being under development, whereas the data center and the business analysis are completed. In view of these considerations, Romania plans to pre-notify the identity scheme as a platform developed within PSCID in January 2023.

Data provided by Member States for the Digital Economy and Society Index [10] show that more than 60% of European citizens have an eID. Cyprus is planning to start issuing an eID as a pilot in the third quarter of 2022, whereas Romania included in their RRP an investment that is expected to deliver 8.5 million eIDs by June 2026.

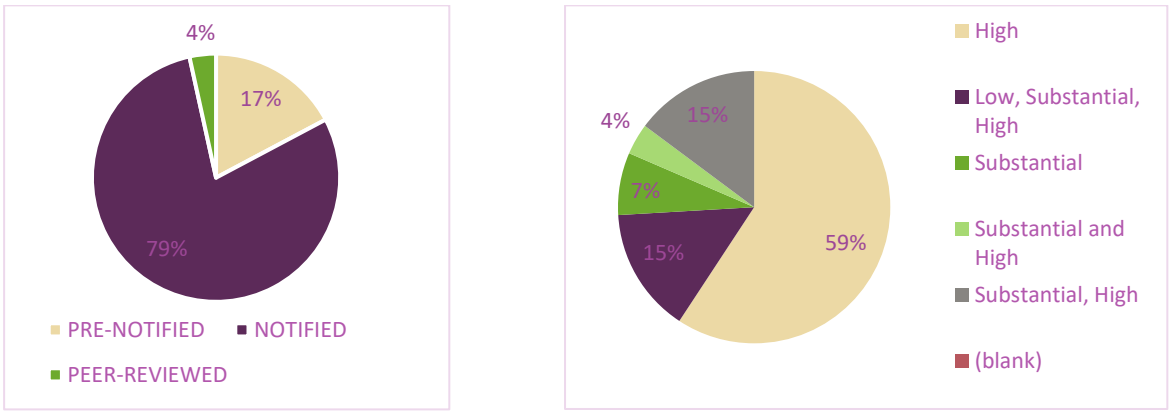

Figure 1: a) Notification status of national eID-schemes b) Level of assurance of eID-schemes

The above results show that, compared to the first phase of data analysis within WP1, there is a significant advancement in both the notification status of the eID schemes, as well as their levels of assurance.

Of the 18 respondent countries, 72% (13) have an eID scheme suitable for cross-border use as well, whereas the others have only national eID schemes (Figure 2). This is somewhat higher extent of cross-border implementation than the one we noticed in the first phase, when 50% of the countries had their eID schemes suitable for cross-border use.

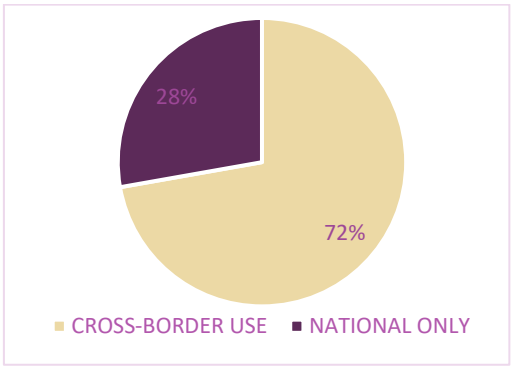

Figure 2: Cross-border use of the eID schemes

In terms of the extent to which they have explicitly laid out and formalized their eID strategy, we find more relevant data from the DESI 2022 report, which showed that Member States can be divided into several clusters [10]:

- Stand-alone eID strategy document: Countries that have developed a dedicated strategy for implementing and promoting eID, identifying objectives and deadlines for new measures. This cluster includes 2 Member States: Denmark and Germany.
- Section of wider digitalization strategy focused on eID: Countries that have dedicated a specific section of their national digitalization strategy to the implementation of eID measures, which could be the development of new eID means, the update of an existing one or the setup of an eGovernment program within which eID plays a crucial role. This cluster includes 16 Member States: Austria, Belgium, Croatia, Cyprus, Estonia, Finland, France, Ireland, Italy, Malta, Netherlands, Poland, Portugal, Romania, Slovakia and Sweden.
- Brief reference to eID within a wider digitalization strategy or strategies: Countries having developed a national digitalization strategy or strategies that makes some mention of eID, but does not expand on this subject in detail. This cluster includes 9 Member States: Bulgaria, Czech Republic, Greece, Hungary, Latvia, Lithuania, Luxembourg, Slovenia and Spain.

However, the above clusters are very dynamic and the state of eID-based services changes rapidly across all countries. For instance, although part of the last cluster, Latvia is one of the few countries in the EU that already provided a unique and president identifier via the eIDAS gateway. In December 2021, the Latvian cabinet of ministers approved amendments to the law on electronic identification of natural persons, according to which public sector e-services must be accessible with notified eID means from other EU countries by 01.02.2023. On the 28th of June 2021 the office of citizenship and migration affairs launched the new natural persons' register introducing a unified approach for registering foreigners (including those who use the eIDAS gateway) providing them with a unique and president identifier therefore allowing them to access Latvian e-services.

Similar to the first phase, service orientation of the eID schemes varies depending on the type of operating entity (see Figure 3). However, the distribution of issuers significantly differs between the two phases, with public entities amounting up to 67% of the eID operators (as opposed to the 56% in the first phase), private entities dropping down to 22%, and the partnership of the two rising to 11% (unlike 7% in the first phase). Although the dataset is far from being exhaustive, these trends can be taken as a relevant signal for an increased collaboration between the public and the private sector. The prevalence of public entities as the operating eID entities is also understandable to some extent, as the implementation of the eIDAS Regulation is yet to be successfully transposed into the national laws of the Member States. Moreover, with its latest revision and the additional technical requirements regarding the new EU Digital Identity Wallets, the leading role of the State among the issuing and the operating entities is even expected. We return to this topic from the point of view of the Digital Identity wallets later in Section 3.1.4.

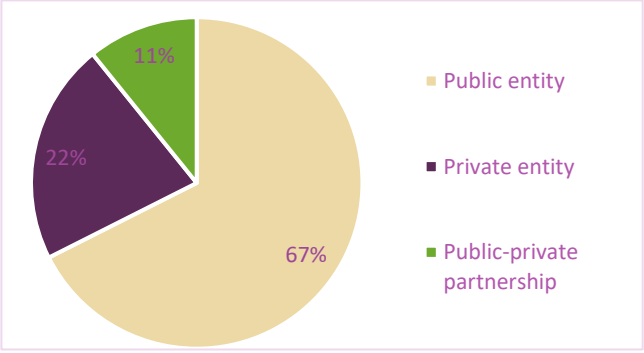

Figure 3: Operating entities of national eID-schemes

One important thing to take from these results is that all the operating entities of eID schemes provide support for a wide set of services. Generally, eID schemes operated by private entities have a higher rate of accessibility to all types of services, including provision of public services at national and subnational levels and various types of non-governmental services. Access to both national and subnational public services are predominantly provided by publicly operated eID schemes, leaving out 40% less for private operators (see Figure 4). Therefore, we often see a case where different public service providers, the single point for access to electronic administrative services and the eIDAS node are integrated within a single electronic authentication system that has been developed specifically for the needs of e-government.

Other important topics to be discussed around the eID schemes are those of transparency, user-centricity and security. Although these are out of the scope of our report, they are important for putting the information given here into the relevant perspective. Therefore, we refer the interested reader to [10] for User centricity and Transparency, to [7] for Security of ID means and to [14] for general future trends of eID.

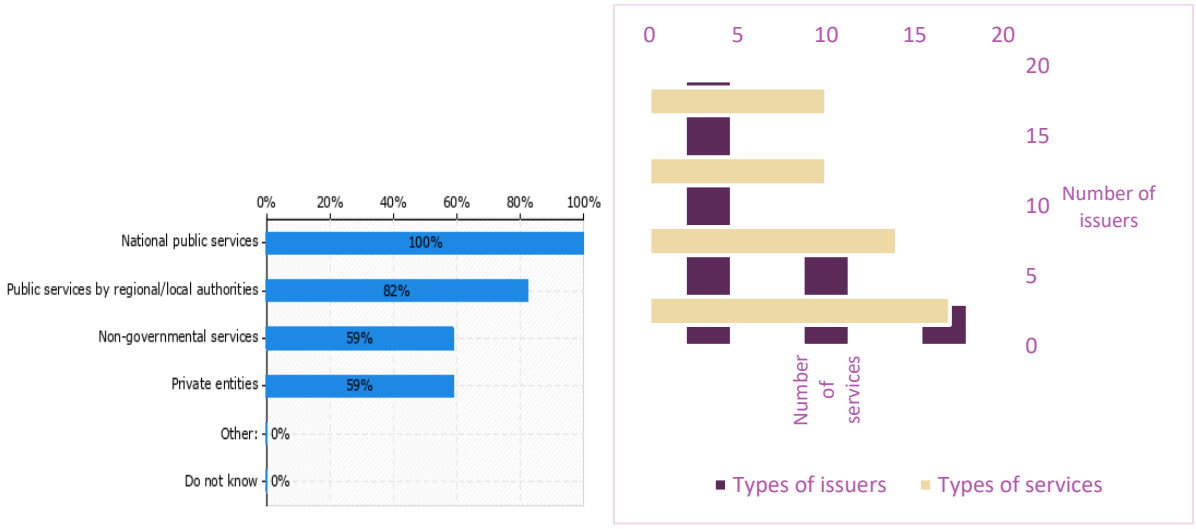

Figure 4: Implementation of access to services depending on the operating entity

From the user's perspective, the DE4A study differentiates three stages of the eID adoption rate:

- ***Possession rate*** demonstrates the share of the inhabitants of the EU Member State, who have acquired an eID scheme. The index is calculated as a total number of holders of the eID mean divided by the sum of the state's population including foreign residents.
- ***Activation rate*** depicts the number of the distributed eID means that was actually activated after receiving it. The rate is calculated as a total number of the activated eID schemes divided by the number of the distributed eID schemes.
- ***Use rate*** represents the share of eID holders who have used the acquired eID scheme at least once to access one of the available services. The index is calculated as quotient of the number of the eID schemes used at least once and the overall number of the distributed eID schemes.

Data obtained on the possession, activation and use rates of the eID schemes is very poor and do not allow for meaningful analysis to be performed. Certainly, these may also be correlated with the eID schemes' operating entities, but our data do not allow for such exercise. We are able to show the distribution of activation and possession rate across countries (see Figure 5), which should be seen only as a trend chart, but not as an informed statistical representation. We were not able to obtain such data for the use rate.

Overall, the reach of the privately operated eID schemes is lower. In certain countries there is a specific law stipulating the mandatory possession of the eID cards as the primary identification document. For example, Belgium postulates obligatory distribution of eID cards among the population reaching the age of 12. Also in Belgium, the specifically designed Kids-eID is optional for the children under 12 years old and can be issued by a corresponding request. Similarly, Portuguese citizen eID card is mandatory for obtaining within the first 20 days after the birth registration, entertaining the strategy of mass use of the eID authentication means. Some other countries enact optional distribution of the national eID cards as a substitute for the existing national passports.

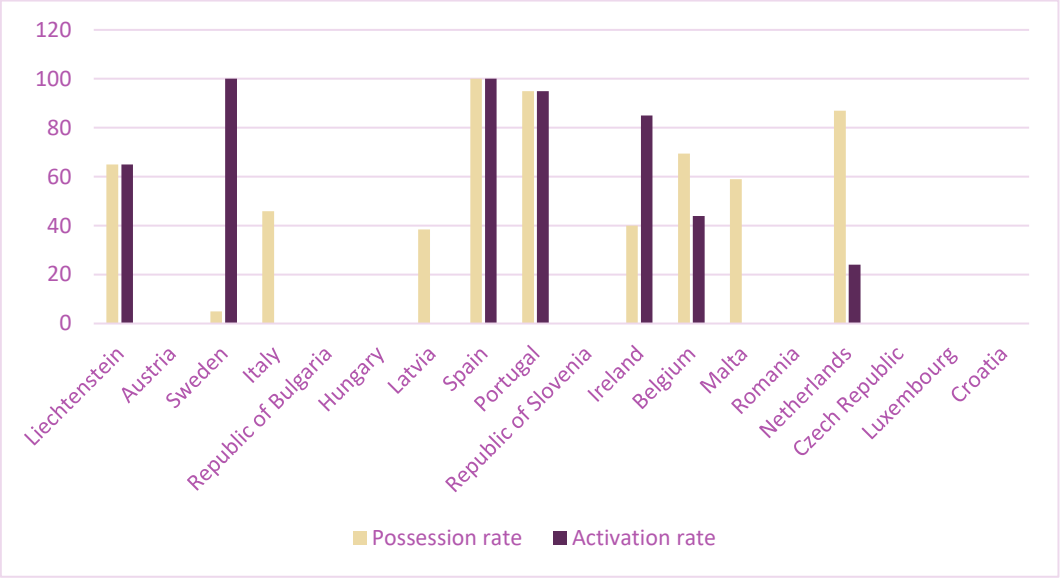

Figure 5: Adoption rate of national eID-schemes depending on the operating entity

Figure 5 represents an overall adoption rate of the studied eID schemes, regardless of their functional purpose (e.g. supplementary mobile solutions or schemes for professional certification). In general, the possession rate of the eID schemes surpasses or is equal to the activation rate, signifying that that are more or equal number of eIDs issued for use than actually being used. In some cases, however, it is the activation rate that is higher (e.g. Sweden and Ireland), implying that once the eID scheme is distributed, it is likely to be activated (Figure 5). Although the eID schemes operated by public entities have considerably higher possession rate than those by private entities, the activation rate for the later in general demonstrates higher values. In that context, to combat the low use rate of public eID schemes, Germany chose to pre-activate the distributed public eIDs, reducing the number of administrative procedures required to commence using the card. From July 2017, the German law also restricted the deactivation possibility for the eID cards. Furthermore, according to the amendments to the personal identification law in Latvia, the eID card will be a mandatory personal identifications document for all citizens from 01.01.2023. National eID means are available free of charge for all citizens. Latvia has no specific eID mean for businesses, only for natural persons. 11 services are available cross-border via the eIDAS gateway and more than 25 (not including business permissions) via the Single Digital Gateway in the state portal latvia.lv. Finally, in Spain every citizen has the obligation to obtain the DNIe from 16 years old. The DNI is a physical card with biometry and a X.509 certificate that can be read with a NFC or a smart card reader. The certificate is valid for at most 60 months and there are standalone digital kiosks in some police stations to activate them by the citizen's fingerprint. This has the effect of both immediate introduction of the citizens to the digital transformation of the government services, and timely harmonization of the national laws and data strategies.

3.1.2 eIDAS-Node

The versions of eIDAS nodes across countries varies from as early as v1.2 to v2.6, with most of the nodes being CEF eID v2.5.

In compliance with the eIDAS regulation, all EU Member States were obliged to recognize electronic identification from other countries when this part of the regulation entered into force in September 2018. Self-assessment reported that 77.8% of the respondent countries have implemented an eIDAS-node for receiving foreign eIDs (see Figure 6). Some of the respondents which reported current unavailability of foreign eIDs recognition noted the readiness of the national eIDAS-Nodes for cross-border user. However, they admit that there is a necessity for supplementary bilateral testing to ensure smooth functioning of the sending and receiving mechanisms.

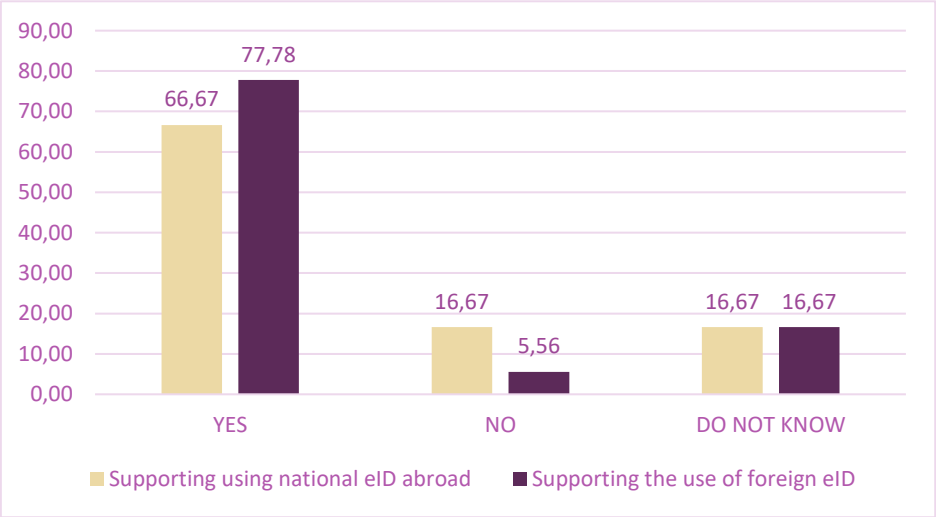

Figure 6: Implementation status of eIDAS-Node

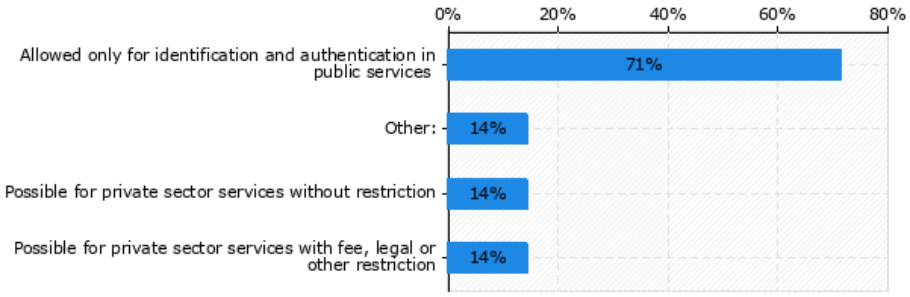

Figure 7: Principle of using / enabling foreign eIDs

As Figure 7 shows, in their support of foreign eIDs, respondents note several principles under which this use is allowed: in 71% of the cases, foreign eID are allowed only for identification and authentication in the process of the obtaining some of the public services in the respondents' countries. Only in 14% of the cases it is possible to use a foreign eID for access to private sector services without restriction, and equally so for access with restriction (with fee, legal or other type of restriction).

Notably, the respondent countries reported higher advancement level of the eIDAS-Node to receive foreign eIDs over national eIDAS-Node supporting national eIDs for foreign use (77.8% against 66.7%). Recognition of foreign eID set as a priority of the eIDAS regulation has determined the prioritization of the eIDAS-node development as well. For instance, the Hungarian node, although not yet in a

production environment, is set for conducting bilateral tests with several Member States: The Czech Republic, Slovakia, Ireland, Italy, and Estonia, and is expected to go live in 2022 Q3. Similarly, the Slovenian eID will perform these test in the beginning of 2023, when the eID scheme is expected to be notified.

3.1.3 Trust services

Trust services included in the eIDAS regulation have implied several stages of implementation, commencing with electronic implementation and then proceeding to advanced and qualified implementation (depending on the type of trust service). Although electronic seal and electronic signature have all three stages, the eIDAS regulation recognizes only electronic and qualified timestamp.

Based on the survey responses, the e-signature has the most advanced level of implementation among the trust services under the eIDAS regulation (see Figure 8). Advanced and Electronic signatures are being widely used for both national and cross-border purposes, with only a small percent of countries supporting only national use. Although to a smaller extent, such is the case with most of the trust services. Exception are the Electronic registered delivery services and the Electronic ledgers. Notably, there is no major consequential dependency between implementation of trust services and availability of the previous step of service implementation – e.g. implementation of *Qualified* electronic timestamp and certificate for website authentication, according to the survey data, are widely spread at national level, while their *basic* counterparts have significantly lower level of adoption.

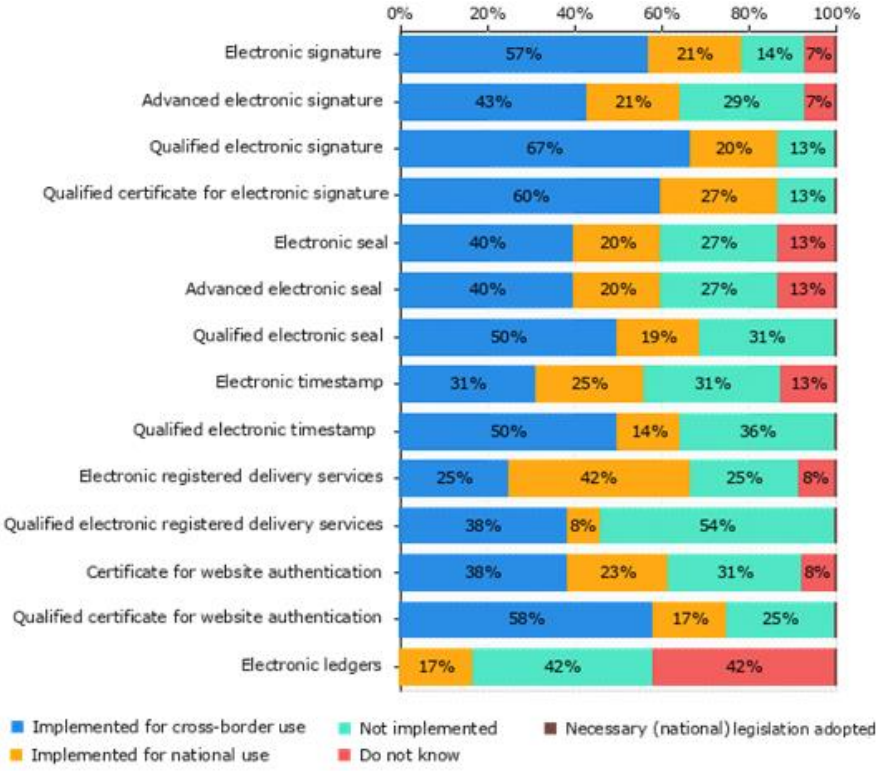

Figure 8: Implementation of trust services

Note: The points of the chart indicating implementation of basic trust services refers to non-advanced trust services. Similarly, qualified services generally comprise advanced trust services with additional quality assurances. Thus, data on advanced trust services should be understood as referring only to non-qualified trust services.

From legislative perspective, not all countries explicitly reference the formats of trust services in their corresponding national laws (for e.g., national regulation omits Electronic Signatures, referencing only

the use of Advanced and Qualified Electronic Signatures). In some countries, there is no dedicated national legislation, which implies exclusive reliance on the eIDAS Regulation, entailing availability for cross-border use. For instance, in Spain the use of the eIDAS node for notified foreign eIDs is already integrated in the Spanish digital identity gateway Cl@ve. Similarly, qualified electronic signatures, seals and timestamps are integrated in the Spanish digital certificate platform @Firma and the Spanish digital timestamp platform and @TS. In the Netherlands, this process is relieved by leaving governments and companies completely free to decide whether they will use trust services and which ones (qualified or non-qualified), without requiring separate legislation or implementation from central government bodies.

Due to the potential for perceived legal uncertainty in that regard, we inquired on the implementation of monitoring mechanisms of the state of eIDAS implementation. This is shown in Figure 9.

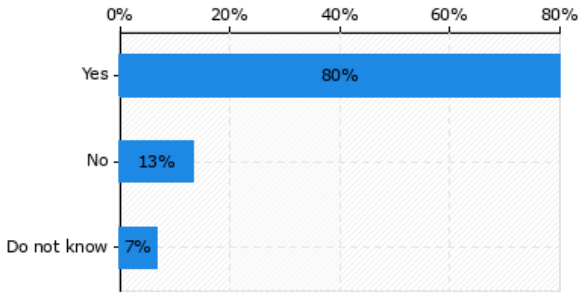

Figure 9: Existing monitoring mechanism on the progress of eIDAS implementation

The results demonstrate high integration of monitoring mechanisms across most of the responding countries. This development address one of the major drawbacks pointed out by the revision of the eIDAS, namely – the poor monitoring mechanisms that exist for eIDAS. Considering the new requirements for developing a Toolbox for the support of the technical system for the revised Regulation, the knowledge base from these monitoring systems can be used in a coordinated manner for various purposes: sharing insights on risks and barriers, as well as good practices that can catalyze the implementation progress.

The monitoring mechanisms are mostly employed (in 92% of the cases) to check whether the necessary changes that go in line with the compliance obligations by the regulated entities have been in place. In additional to overview the extent to which the changes have been implemented, 83% of the responding countries report monitoring indicators in place to measure the extent to which this implementation is in line with the adopted measures. Finally, as part of the monitoring process there are also mechanisms that overlook the sector-specific implementation of the necessary changes, in 67% of the cases.

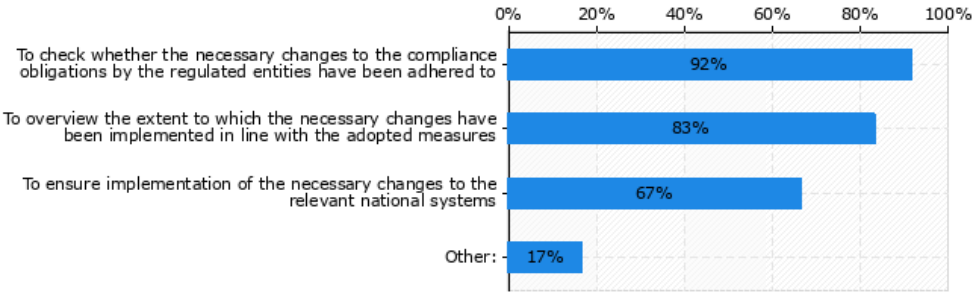

Figure 10: Purpose of monitoring mechanisms

Countries also reported significant inhibition to the technical implementation of eIDAS due to the pandemic, while at the same – higher demand for eID and eGovernment services. The main barriers to the implementation of the eIDAS elements (nodes, schemes, and trust services) have been: reluctance to adaptation and change by both public and private sector (including citizens), small timeframes to implement the changes, lack of digital skills and human resources, as well as frequent changes in the governance structure due to fluctuations (during the pandemic). Some of these hurdles still persist, especially in terms of the adaptation of the national laws.

However, most of the developments have now been restored and are catching up with the requirements of the revised Regulation.

3.1.4 Digital Identity Wallets

Although the adoption of eIDAS has been progressing since the start of its implementation, there are important aspects of it that hinder its adoption [15]. As the beginning of the eIDAS transposition into national laws was marked, wide monitoring and evaluation practices followed the progress of its implementation. By 2021, the Impact Assessment of the implementation progress of the eIDAS Regulation has identified four major problems in that regard:

1) Increased demand by public and private services for trusted identification and exchange of digital attributes is not met;
2) Current user expectations for seamless and trusted solutions to identify and share attributes across borders are not met;
3) Data control and security concerns are insufficiently addressed by available digital identity solutions; and
4) Unequal conditions for the provision of trust services and insufficient scope of the Regulation.

In addition, the integration of authentication systems into web services is complex, and authentic interoperability between notified schemes has not been achieved. One of the objectives of the eIDAS revision is to improve this interoperability and transaction by introducing the European Digital Identity Wallet (EDIW), which will allow its users to access online services, share electronic documents and identify themselves throughout Europe, with full control over the data shared.

In addition to revising the eIDAS Regulation, the European Commission and the Member States has been preparing the ground technically and infrastructural as well. Thus, the European Blockchain Services Infrastructure (EBSI) aims to address the above challenges from several perspectives [16]. As this effort tries to bring greater data control to citizens and businesses over their data, the participation of the GovTech ecosystem is more crucial than ever before. It is therefore of paramount importance that we note increased public-private partnerships around the establishment and operation of eIDAS schemes (see Section 3.1.1). Once all the infrastructural elements are in place, it will greatly accelerate the dissemination of emerging technologies in everyday applications connecting governments to their citizens.

From Figure 11 and Figure 12, we see that most of the responding countries have not established a Digital Identity Wallet solution yet. However, most of them (40%) have also been considering it as part of the electronic services offered to the citizens. With the introduction of the eID, Liechtenstein has started implementing several projects on digital identity wallets and has already 3 solutions (eAusweis, eFührerschein, and Alters-Check), all at prototype stage. In addition, an effort on establishing a digital driving license is under way. This creates an optimistic view on the future development of the DIW solution and their integration with current technical and regulatory practices. Furthermore, Luxembourg has the national eWallet already in production, as is the case with Portugal as well.

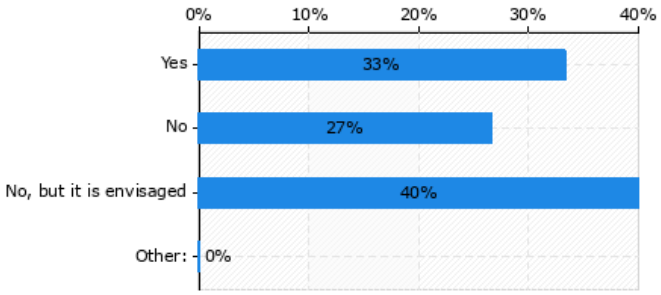

Figure 11: Existing National Digital Identity Wallets

Currently, the Spanish law does not support self-sovereign identity means, but has been taken under consideration as a desirable approach for the future. Spain is also a leader in some EBSI groups and pilots, along with other blockchain initiatives to develop the potential of the new approach.

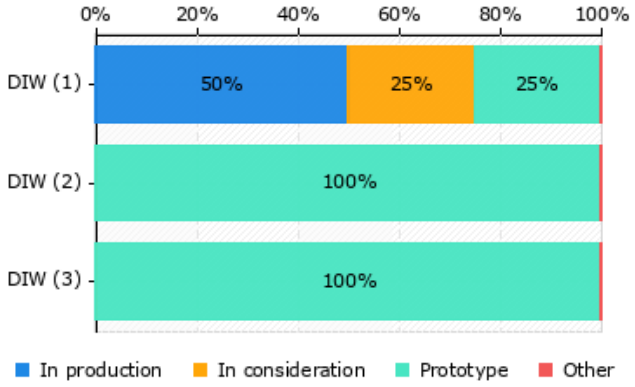

Figure 12: Stage/form of implementation of the solution

All reported DIW solutions have been issued by public entities. The validation mechanisms for the digital identity wallets provided by the state have been mainly in the direction of ensuring that their authenticity and validity can be verified, to allow relying parties to verify that the attestation of attributes are valid, and to allow relying parties and qualified trust service providers to verify the authenticity and validity of attributed person identification data. This is presented in Figure 13.

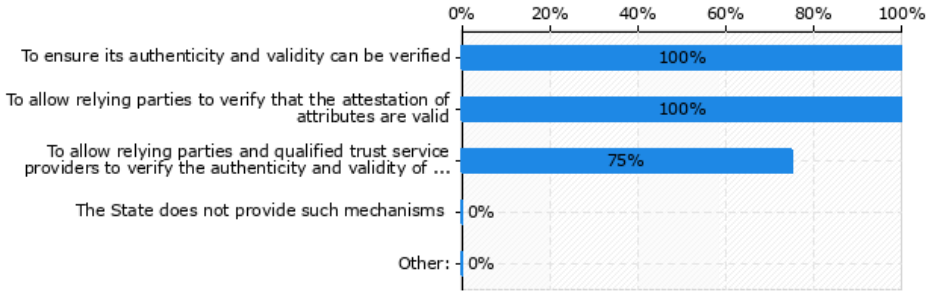

Figure 13: Validation mechanisms for the Digital Identity Wallets provided by the State

All DIW solutions provide means to ensure that the DIW is free of charge to natural persons. In addition, there are accredited bodies that certify the conformance of the DIWs with the requirements laid down in the relevant paragraphs of article 6a) from the eIDAS v2.

Currently, there is no legal obligation for Member States to implement an EU Digital Identity (EU DIW) Wallets. However, as some solutions do exist, they often represent some kind of a transition model for

moving towards the regulatory practice, which may facilitate the migration of the technical infrastructure and the overall adoption of the European Digital Identity Wallet as prescribed by eIDAS v2.

Nevertheless, from our experts' interviews, we find that:

"…it may also be the case that some of the current solutions become redundant with the transition to complete EUID Wallets. This is also a reason for certain tensions between the private and public sector, with the latter demanding clear representation of its interests from the inception of the regulatory planning and efforts. At this stage, a clear transition model is needed to guarantee that current solution will not become redundant with the introduction of the revised eIDAS Regulation." **– EBSI expert**

From an infrastructural point of view, the digital wallet depends on several technical elements:

- The first element is a fully functioning, permissioned, but publicly available, blockchain network that can be trusted by European public administrations. This involves, among other things, strong governance arrangements and security controls;
- Second, a digital identification framework is a crucial prerequisite for this pattern to work. In a typical blockchain paradigm, this means that every public administration, business and citizen would need to get a "decentralized ID" (DID). DIDs are a new type of identifier that enable verifiable, decentralized digital identity.
- As DIDs say nothing about the actual person or organization associated to it, a scalable solution is needed to link DIDs reliably to their associated 'legal' entity;
- Finally, citizens and businesses would need to have a trusted and secure digital wallet, connected to the blockchain, to hold their DID and documents.

At this point, it remains to further follow the progress of the implementation of the new and see how it plays out, especially in terms of establishing interconnection with the rest of the regulatory developments, notably the OOTS and the SDG.

3.2 Digital Service Infrastructures

Consolidating reusable blocks of infrastructure, the Connecting Europe Facility (CEF) establishes a set of sector-specific and building-block DSIs, which can later be deployed by Member States in their national eGovernment initiatives. To improve cross-border interoperability, the CEF Digital programme recommends using the developed building blocks in respective national solutions. Relevant for different utilization domains, the DSIs have been implemented to a different extent throughout the EU. The reference system for measurement of the DSI implementation by different countries includes their overall intention of the use of the listed DSI and the status of its practical implementation.

The two major initiatives that DE4A benefits from are OOP and SDG, whereas the projects with whom the most interdependencies can be established are: TOOP, SCOPP4C, the Estonian Catalogue of Public Sector Information, CODEX (Evidence2E), e-SENS and STORK. All of these rely on the use and reuse of certain EU Digital Service Infrastructures themselves, which are summarized by the extent of implementation by other countries and projects in Table 1. The data in the table has been extracted from information obtained from the CEF monitoring dashboards.

Table 1: Implementation of Digital Service Infrastructures across countries

EU DSI	Implementation
eArchiving	**4** projects / **11** countries, **22** implementations or proofs of concept, 10 countries' national archives

EU DSI	Implementation
eDelivery	**23** projects in **20** countries, **680** access points across **39** countries
eID	**72** projects / **26** countries, **25** countries deployed an eIDAS-Node that passed the interoperability readiness test
eInvoicing	**49** projects / **27** countries, **72** B2G solutions which successfully passed the EU Testing validation (conformance test)
eSignature	**72** projects **/ 26** countries
eTranslation	**29** projects / **29** countries
European Blockchain Services Infrastructure (EBSI)	**29** countries, including the **27** Member States, Norway and Liechtenstein, signed the EBP declaration.
Public Open Data (including both Big Data Test Infrastructure and Context Broker)	**40** projects / **27** countries, **20** organizations / **17** countries at the time of data collection
Business Registers Interconnection System	**10** countries, **16** agreements have been awarded to BRIS
Cybersecurity	**100** projects / **28** countries, **More than half of all Member States** are involved with a given area of the EU Cybersecurity Strategy
Digital Skills and Jobs Platform	**26** countries, National Coalitions are present in **23** Member States
eHealth	**26** countries, **953** healthcare providers actively participating in European Reference Networks
Electronic Exchange of Social Security Information	**28** countries, **All the Member States** are connected to the Central Service Node through access points
eProcurement	**20** countries, **89** ESPD or eCertis service implementations
Europeana	**26** countries, **24** Generic Services Projects
European Digital Media Observatory	**18** countries, **8** Generic Services Projects
European e-Justice	**27** countries, **All Member States** participate in the European Court Database
EU Student eCard	**17** countries, **8** Generic Services Projects to promote student mobility
Online Dispute Resolution	**3** projects / **3** countries
Safer Internet	**30** countries / **114** Generic Services Projects **158 countries**, including **26 Member States**, participated in the **Safer Internet Day (SID) 2019**
Broadband	**3** Broadband infrastructure projects

EU DSI	Implementation
WiFi4EU	27 Member States, 2 European Economic Area (EEA) countries and the United Kingdom. More than **8,800 European municipalities** participate in WiFi4EU

The implementation and maintenance of the DSIs, in turn, depends on the types of building blocks that are being (re)used for the various sectorial needs. The reuse and uptake data for each of the building blocks was until recently maintained and updated by the CEF (see Figure 14), but has now been migrated to EC premises [17].

The results from the first phase show high access (from 90 to 100%) to reusable public sector information, eInvoicing, eDelivery demonstrate one of the highest implementation scores, along with sector-specific DSI such as BRIS, eProcurement, and e-exchange of social security. On the other hand, EU student card, Online Dispute Resolution (ODR) and Automated translation showed considerably lower level of advancement. However, within their relevant contexts, the employment of the latter DSIs have also been on the rise, with eTranslation being employed in 29 projects across 29 countries and EU student card across 17 countries. ODR is slowly getting pace, with 3 countries using it as part of 3 projects.

Figure 14: Reuse matrix of CEF Building Blocks across Digital Service (and Sub-service) Infrastructures

In order to get a DE4A relevant perspective of the use and reuse of building blocks, liaison was needed with the other project partners. Several consultations were held for that purpose, after which the interconnections with WP2 shown to provide the bulk of the information. The results from these consultations are summarized in Table 2 (showing the use/reuse of building blocks in view of the relevant project stakeholders) and discussed in continuation.

Business Registers Interconnection System (BRIS) enables cross-border functioning of the companies, allowing them to benefit from the Digital Single Market. Envisaged by the Directive 2012/17/EU, the European Commission stipulated obligatory interconnection of companies' registers in order to create a more adaptive environment for businesses. Introduced in June 2017, BRIS registers the information on companies – e.g. legal form, representatives, annual accounts – and makes it accessible within the EU shared market. In the first phase, it was found that all respondent countries have to a certain extent initiated technical implementation of the BRIS at their national scope. Being closely connected to eDelivery and eJustice DSIs, BRIS conditions the development of the associated building blocks. In the context of DE4A, BRIS has some overlap with the use cases in the Doing Business Abroad (DBA) pilot, both in relevant authorities (i.e. business registers) and in exchanged information. Even if BRIS can only be used by (a subset of) business registries themselves, it already provides today an operational exchange of company information across Europe. A reuse of (an extended) BRIS is understandable in the interest of the participating business registers, however, the possibility of DE4A to create legal and technical changes on the existing BRIS system is very limited. Analysis of the DBA pilot shows that the potential of reuse of BRIS is limited for the pilot, i.e. will remain at the level of the reuse of data definitions[1].

Table 2: Reuse of building blocks in DE4A

#	Building Block	Used	To be assessed by
	Common Components		
1	eDelivery	yes	WP5/MSs
2	SMP/SML	yes	MSs via pilots
3	DE4A Connector	yes	MSs via pilots
4	DE4A Playground	yes	WP5/DBA/SA/MA
	Semantic		
5	Information Exchange Model	yes	DBA/SA/MA
6	Canonical Data Models	yes	DBA/SA/MA DE and DO pilot partners
7	ESL (implemented as part of SMP/SML)	yes	WP5
8	IAL	yes	WP5
9	MOR	yes	WP3/WP5/MA pilot partners
	eID/PoR		
10	SEMPER	yes	DBA
	TOOP	no	(only parts of the TOOP Connector software architecture was reused as a shared library)
	VC Pattern		
11	SSI Authority agent	yes	SA
12	SSI User agent (mobile)	yes	SA

[1] For more information, please see: https://wiki.de4a.eu/index.php/Doing_Business_Abroad_Pilot

13	EBSI-ESSIF (CEF Blockchain)	yes	WP5

In the context of using Blockchain technology, there were several legal concerns related to the use of Self-Sovereign Identity, such as the storage of personal data in distributed ledgers or the validity of a decentral identifier. This led Spain to entirely ban blockchain from application in eGovernment. By RDL 14/2019, it is forbidden to use a blockchain infrastructure to offer any identification or signature process (until a European or national law regulates the use of these technologies). Ongoing research, discussions, and progress in context of EBSI and ESSIF are clearly relevant for DE4A. It cannot be ascertained yet whether piloting use cases applying blockchain technology can go live in production or would remain exploratory, running in acceptance environments.

Electronic Exchange of Social Security Information (EESSI) is a domain specific, sectoral network that has some overlap with one of the use cases in the DE4A Moving Abroad (MA) pilot, i.e. Request Pension Information & Claim Pension - both in regard to relevant authorities and to exchanged information. The MA pilot had been assessing some EESSI capabilities for reuse. This reuse can take different forms - from full adoption of EESSI for the use case to the adoption of harmonized data models and definitions.

Additional information of relevant initiatives and project whom DE4A finds reusable elements from can be found in the WP2 deliverable on the second iteration of the project start architecture, D2.5 [18].

For the general European landscape, it can be concluded that the efforts toward DSI implementation are widely distributed, with a small number of DSIs going through a slower take-up.

3.2.1 Blockchain-based solutions

The adoption of blockchain technologies is associated with a considerable potential for public sector transformation. Aiming to increase transparency and accountability of the interactions among the government, businesses and citizens, the EU Digital program acknowledges blockchain technologies as one of the underlying building blocks [16]. The joint efforts of the European Commission and the European Blockchain Partnership resulted in the creation of the European Blockchain Service Infrastructure (EBSI), which connects the nodes across Europe and provides reusable solutions to support the adoption of blockchain-based solutions by European public authorities.

As show on Figure 15, more than half of the countries report participation in use cases led by EU funded efforts on blockchain. A list of particular use cases also can be found in the deliverable D1.6 Updated baseline for EU building blocks.

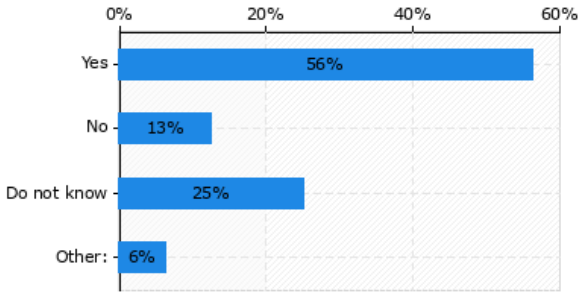

Figure 15: Countries' participation in EBSI, H2020, CEF Digital or RRF projects' use cases

Pilot blockchain projects on Notarization, Diplomas, European Self-Sovereign Identity and Trusted Data sharing were launched in 2019. Notably, Self-Sovereign Identity (SSI) is among the most frequent blockchain solutions among the respondent countries. Expected to change the centralized approach of managing one's identity data, SSI provides the users with the possibility to store this information at

their side. The European Self-Sovereign Identity Framework coordinated by the European Blockchain Service Infrastructure and by the European Blockchain coalition, sets governance frameworks for national implementation of the SSI by its Member States. The Netherlands, being one of the pioneers in the domain of SSI, develops its solutions under the cascaded EU project on European Self-Sovereign identity Framework (ESSIF) that is expected to be coupled with the existing eID schemes (e.g. DigiD [19]) and which is being assessed in conjunction to the revision of the eIDAS framework [20].

Although the blockchain solutions report by the respondent countries are domain-specific and nationally bound, they are being developed across consistent domains. Housing markets, supply chains and university certificates are among the most spread areas for blockchain implementation. For instance, in December 2019, Spain launched the BLUE project, which incorporates blockchain-based validation of certificates for 76 Spanish universities. Reducing the possibility for altering the certificates via distributed tamper-proof ledger, the Spanish government ensures integrity of the issued diploma and facilitates countrywide and cross-border recognition of national education. Similarly, the Maltese Ministry of Education and Employment has been providing blockchain-based education certificates since 2017. Ensuring the validity of the issued academic certificates for the students and enabling receipt of blockchain accreditation certificates for education institutions, the Blockcerts project has been a useful practice for the DE4A Studying Abroad pilot.

3.3 Single Digital Gateway: Life events

The 21 life events enumerated in the Regulation encompass the most vital services provided by public authorities and are expected to be set on digital track as a high priority. Embodying the principles of user-friendliness, Once-Only, digital by default and other principles of the Tallinn Declaration, the SDG regulation sets a baseline for general public sector transformation and the implementation of these services in particular. To take stock of the current level of implementation of the life events, they were analyzed from the perspectives of eID-accessibility, mobile accessibility, principles of data reuse and availability of the services on a cross-border perspective.

The four parameters – “Means of authentication”, “Mobile accessibility”, “Appliance of OOP (data reuse)” and “Cross-border availability” are represented in the following charts (Figure 17, Figure 18, Figure 19, and Figure 20).

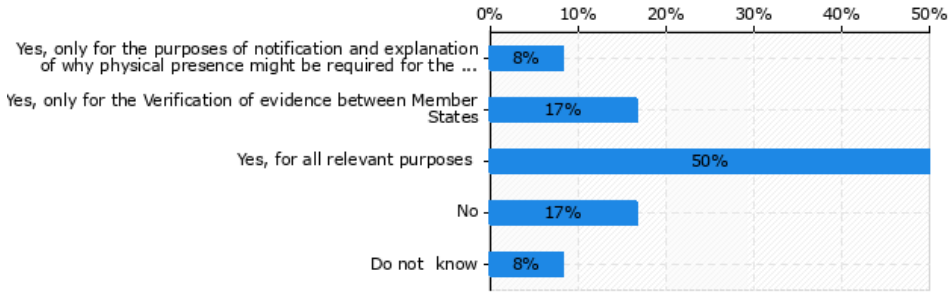

Figure 16: Countries employing the Internal Market Information System

As many of these specificities are defined by the countries’ national laws, their implementation is highly context dependent. Therefore, it is hard to draw any conclusions in terms of assessing the success of their adoption or their implication on the general OOP system.

From Figure 17, it can be noticed that most of the SDG procedures demonstrate high percent of online availability. This percent varies between 71% - 100%, depending on whether the procedure is eID-enabled or not. While most of the SDG procedures do offer the possibility for using eID (from 33% in the case of EHIC, to 83% in the case submitting income tax declaration), there is still high level of eID disabled procedures. Seven procedures require personal presence in order to be carried out

successfully, which differs between countries and among competent authorities. In those cases, most of the countries make use of the Internal Market Information System (IMI), established by Regulation (EU) No 1024/2012: for the purposes of notification and explanation of why physical presence might be required for the "fully-online" procedural steps (Article 6(4)), as well as for the Verification of evidence between Member States (Article 15).

As Figure 16 shows, only 17% of the countries do not employ the IMI, whereas half of them make us of it for all relevant purposes. 8% use it only for notification and explanation purposes, whereas 17% - only for verification of evidence between MSs. The major (50%), however, uses it for all relevant purposes.

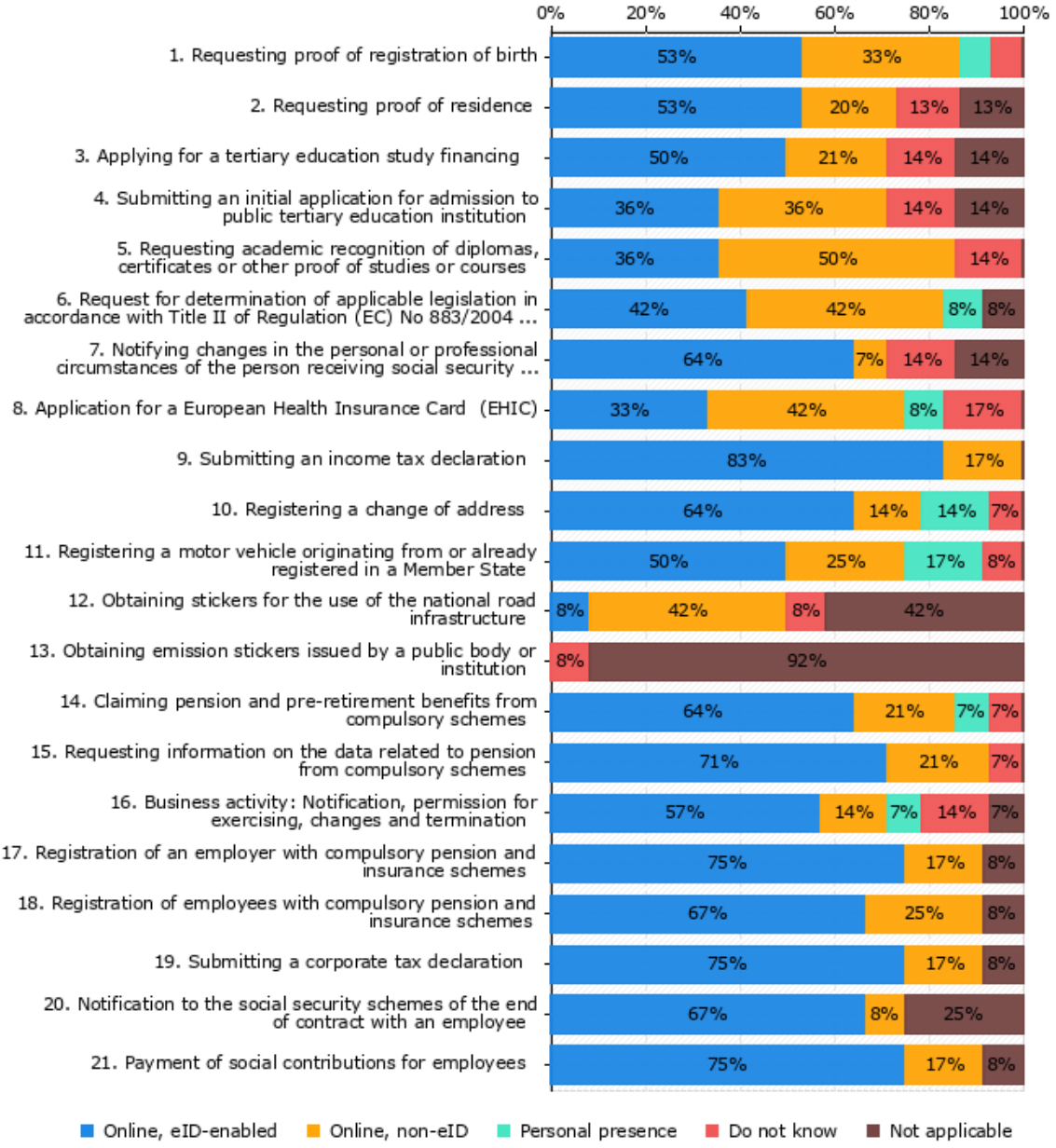

Figure 17: Means of authentication

It is important to note that countries with a federated government – such as the Netherlands, Belgium, etc. – provide regional and local public authorities with a certain degree of liberty in the provision of public services, removing national constraints for developing digital solutions. Hence, countries with

higher autonomy of regional and local public authorities might have different approaches toward the development process, which might lead to uneven results even in the context of one country.

Life events associated with tax collection – namely, "Submitting an income tax declaration" and "Submitting a corporate tax declaration" – have a distinctly higher implementation levels than other services. Compared to the other life events, tax collection is centralized at the federal level, which in its turn contributes to the consolidated approach toward the service development. In the centralized states, the processes are streamlined from the national onto subnational level. On the contrary, countries with federal structure – despite relative freedom for regional and local public authorities – have centralized centers for tax collection, conditioning the unique approach toward the tax-related processes onto lower administrative levels.

While the SDGR approach is relatively clear and pragmatic, there are some inherent complexity stemming from its interdependencies with other technical systems and national legislations. One such insularity come from the fact that the Regulation envisages that the procedures can be completed in a fully online manner (Article 6), meaning that:

- the identification of users, the provision of information and supporting evidence, signature and final submission can all be carried out electronically at a distance, through a service channel which enables users to fulfil the requirements related to the procedure in a user-friendly and structured way;
- users are provided with an automatic acknowledgement of receipt, unless the output of the procedure is delivered immediately;
- the output of the procedure is delivered electronically, or where necessary to comply with applicable Union or national law, delivered by physical means; and
- users are provided with an electronic notification of completion of the procedure.

Thus, an important legal prerequisite is that users can be identified electronically, that they can obtain the relevant evidence electronically, and that they can submit it electronically. From what was discussed above, it is hardly the case at present that these requirements are met. Moreover, the SDGR makes no clear provision on how such state should be resolved in practice.

In terms of Mobile accessibility, Figure 18 presents a relatively positive picture, with accessibility ranging from 40% to over 80%. Although the uncertainty introduced by the "Do now know" responses affects the clarity of the distribution, there is sufficient feedback with high certainty that allows us to still draw meaningful conclusions. Only six of the procedures can be carried out through a dedicated eGovernment app. Furthermore, there are still countries (between 1 and 3 on most of the procedures) that have only desktop-enabled website as the available means to carry out the procedure online.

However, from what we see in Figure 19, the overall cross-border availability of SDG procedures is relatively high, ranging from 50% to 83%, with 14 of the procedures are even higher than the 60% mark. For 13 of the procedures, between 9 and 11 countries have reported having the services available for cross-border use, with the exception of Obtaining emission stickers issued by a public body or institution (with 18% availability and mainly stated as Not applicable) and Obtaining stickers for the use of the national road infrastructure (with 45% availability).

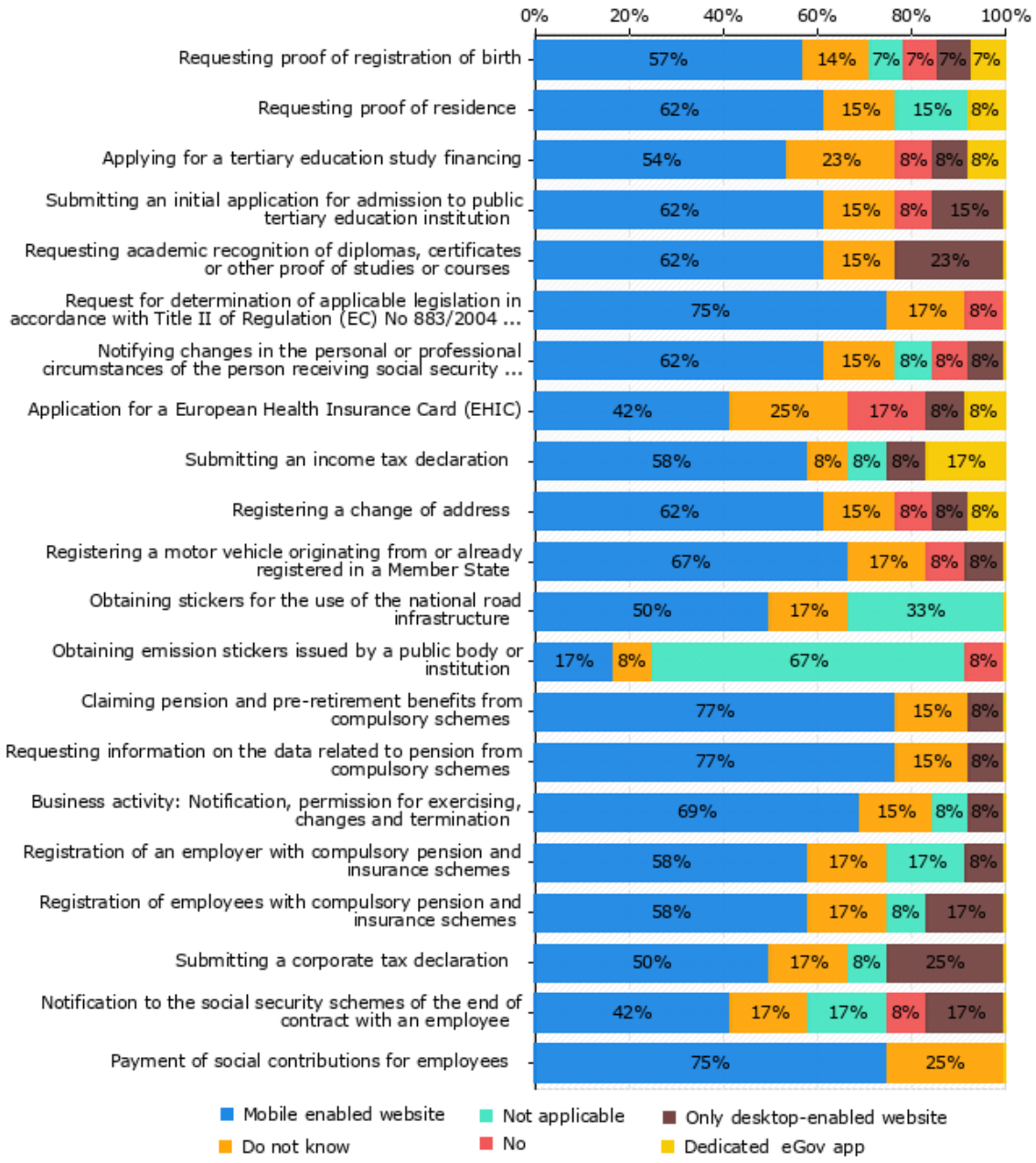

Figure 18: Mobile accessibility

With typical implementation rates in the 30-45% range, the general picture of the implementation of the OOP for cross-border services is one of advanced adoption and implementation. However, it is still insufficient for an effective implementation of the SDG in general. It is important to note that, as the distribution is also relatively skewed due to the uncertainty of answers (where respondents "Do not know"), especially for procedures #5 (Requesting academic recognition of diplomas, certificates or other proof of studies or courses) and #6 (Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004(I)), the previous numbers may actually be higher.

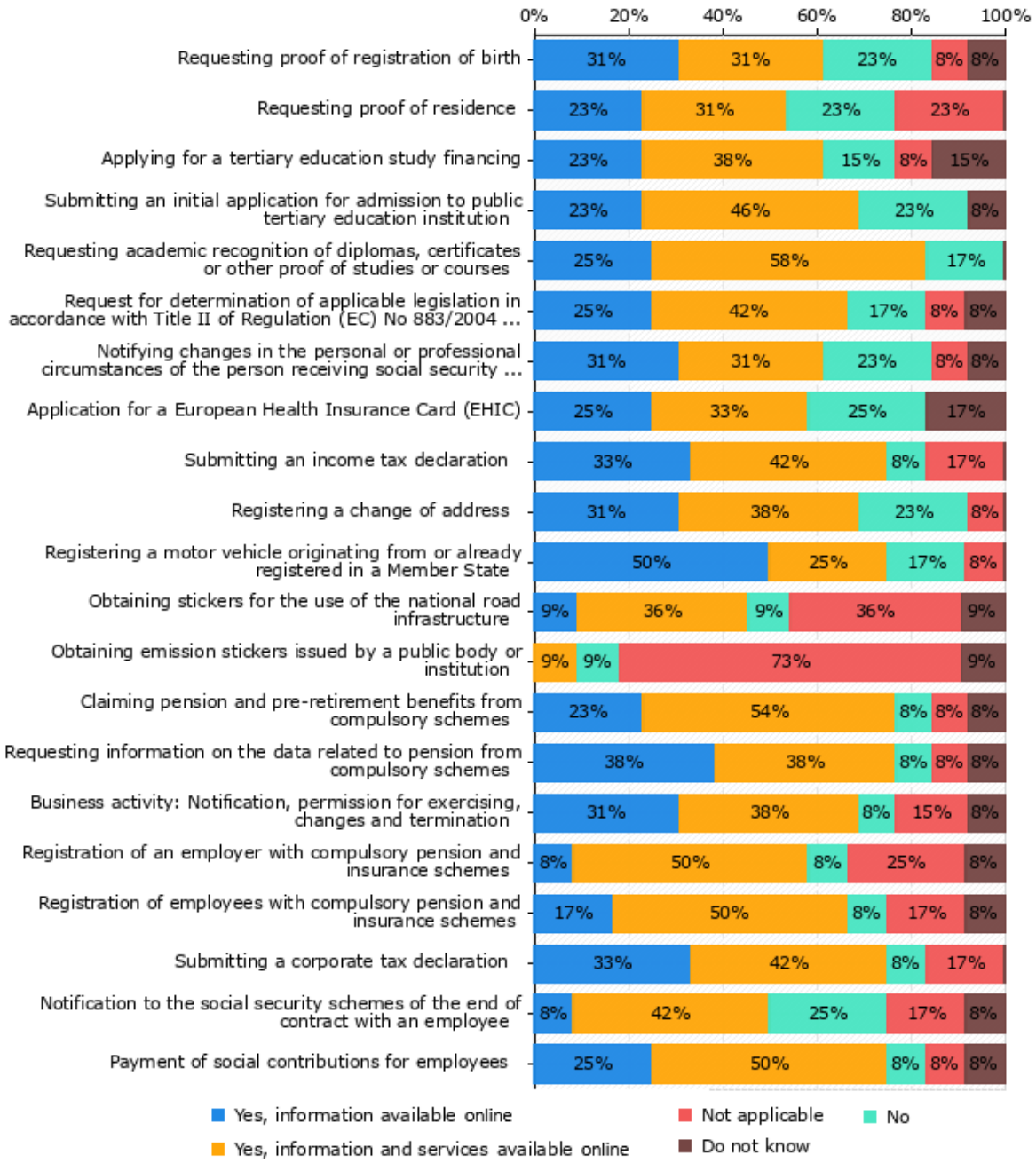

Figure 19: Cross-border availability

Figure 20 shows that implementation of once-only in the 21 life-events has in general been advancing. From DE4A aspect, this advancement is relatively positive in the context of everyday citizen affairs (relevant for the Moving Abroad pilot), and to a much less extent in the business and educational context (relevant for the Doing Business Abroad and Studying Abroad pilots). More concretely, the use of OOP in either unstructured or structured format typically totals to 30-50% for everyday citizen affairs, and between 15-30% for business and education context. Of those that have implemented once only, the choice of implementation is typically reuse of structured data. Furthermore, the raw data reveals that it is only a small subset of countries that accounts for the biggest number of instances when unstructured data is being used. Hence, from (re)use of structured data is the prevalent way of implementing the OOP across all the countries.

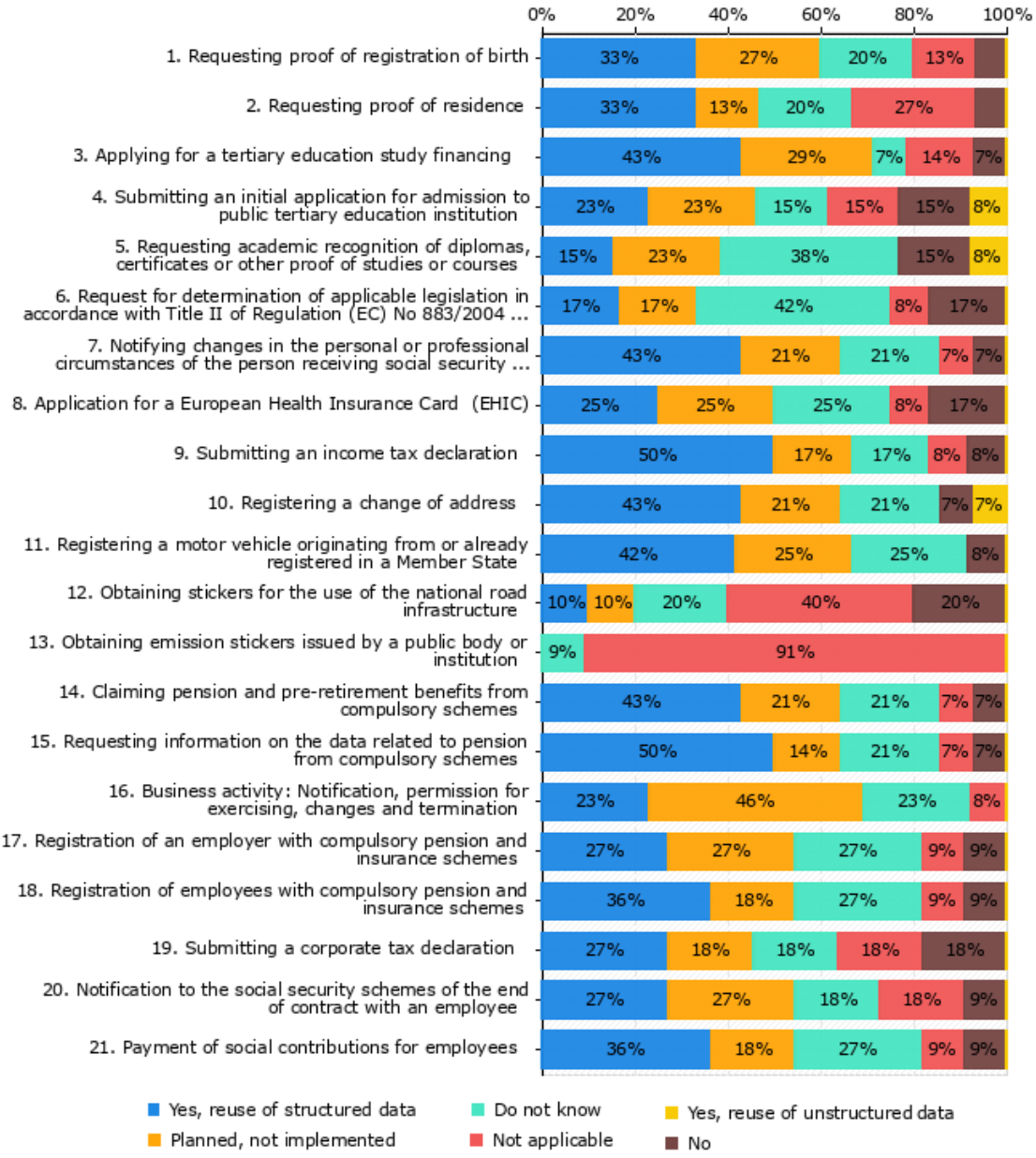

Figure 20: Appliance of data reuse principle

Relatively high percent of respondents (25-30%, and up to 46% for procedure #16 Business activity: Notification, permission for exercising, changes and termination) still report having planned, but not technically implemented the OOP system. Per procedure, the number of countries answering "No" is typically 1-3 countries. However, not all procedures are applicable in every country, which is somewhat expected for a diverse administrative and legal landscape as the European. For the majority of procedures between 2 and 5 countries have reported them as Not applicable, with two procedures standing out: Obtaining stickers for the use of the national road infrastructure (with 40%) and Obtaining emission stickers issued by a public body or institution (91%).

Clearly, the SDG implementation levels across countries vary depending on the overall readiness for digitalization. As a result, some of the countries do not even see SDG as a priority. Such case is Spain, where due to the small percent of cross-border transaction, in addition to scarce human and technological resources, competent authorities are mainly focused on more urgent matters related to

the national users' needs. On the other hand, simultaneously with the implementation of SDG procedures and OOTS, Italy is working on the implementation of PDND (The National Digital Data Platform - "Piattaforma Digitale Nazionale Dati"). It is a secure and standardized framework for the acquisition, control and redistribution of data, which uses a Catalog and Ontology Service, and segregates Data into Organizations, Roles and Access Groups. It will enable single administrations to communicate and share data and APIs in a free and open way, allowing for the creation of new and previously unthinkable services and data applications, realized on the basis of the needs of the citizen. Such developments intertwine with the SDG in a beneficial way, accelerating the implementation of the OOP and contributing to law harmonization as well. Similarly, in Bulgaria, the e-Government Agency has been implementing the project "Upgrading the Single Portal for Access to Electronic Administrative Services with New Functionalities, Ensuring Its Working Capability and Creating New and Updating Existing Templates on Administration Sites", which includes requirements for the services catalog activities, and optimization of the taxonomy of services in the Portal. This should contribute to data harmonization, catalyzing the concurrent OOP activities in the country.

While there are no major differences in the overall implementation level of the services based on the four parameters for most of the services, there are several processes that are lagging behind in comparison to the overall advancement. Registration of a motor vehicle, application for the European Health Insurance Card, notification of personal and/or professional changes, change of address, request for diploma recognition and application for a public education institution score seemingly less than other services. The later three services are use cases in DE4A pilots. With a minor variation, these services primarily yield availability of eID-authentication and principle of data reuse to the remaining life events.

The DE4A pilots oriented on moving, studying and doing business abroad are differently affected by the current development status. While business-related events such as notification, obtaining permission, changes and termination of business along with the live events related to taxation and employment regulation are fairly well implemented, the life events induced in the processes of studying and moving abroad are lagging behind the general levels of implementation of the SDG life events. The process of application for an education institute and change of the address are primarily processed by the regional and local public authorities, which might be associated with a possible lack of centralized coordination, conditioning comparatively lower level of implementation and data reuse.

3.3.1 Digital-by-default

The responding countries have consistently reported the problem of law harmonization, having to adjust, change, or put in place new laws and recommendations to establish the ground for equality of digital and offline service provision. For instance, imposing the legal obligation to provide both offline and online communication channels with the public administration, Austria passed the right to choose the most convenient communication method to the end-user. As a results, the state incentivizes businesses and citizens to explore more innovative channels of interaction with the authorities. In line with the national and European digitalization agendas, 81% of the country respondents noted the presence of a national strategy for availability of public services online.

While some countries adopted a multi-channel approach, safeguarding access to the public services through different channels, several countries demonstrate a rather proactive approach toward service provision. Prioritizing OOP and user-centricity at the base of the public service development, most of the countries scored high in the DESI and eGovernment benchmarks, with Malta being the leading in both user-centricity and transparency of services [10][2]. The status on cross-border service provision, on the other hand, is somewhat weaker, with eID being the lowest scoring indicator[3].

[2] See page 73, Figures 73-76 of [10]

[3] Cross-border eID in the DESI report is defined as the extent to which eID can be used for service processes by users from other European countries; a government-issued document for online identification and authentication.

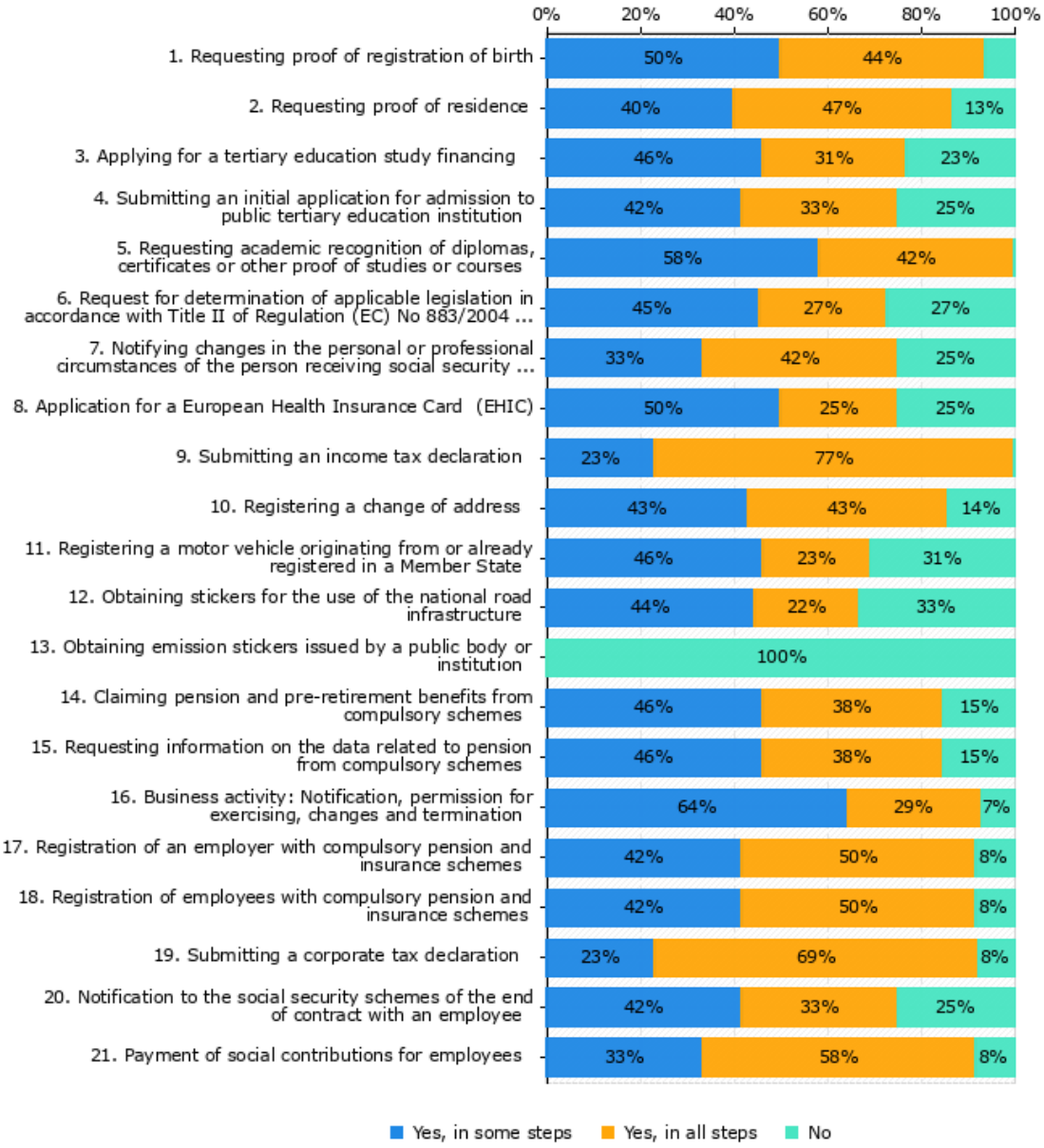

Figure 21: Digitalization of SDG procedures

It is worth noting, in the context of the SDG, digital availability of public services does not imply that there is possibility to carry out a procedure in a fully digital manner. Therefore, we inspect the countries' level of digitalization of each of the SDG procedures. While Figure 21 demonstrates a relatively high digitalization levels for all procedures, none of the procedures has shown to be fully digitally enabled. However, all of them are either fully digitalized, or only in some steps. Interestingly, the lowest digitalization levels can be noted with the two procedures related to submitting tax declaration, which, on the other hand, have shown previously to have a distinctly higher implementation levels than other services.

It is worth underlining that the SDGR's provisions on the OOP do not require digitization of evidences and the underlying procedures. Article 14.2 notes *that "where competent authorities lawfully issue, in their own Member State and in an electronic format that allows automated exchange, evidence that is relevant for the online procedures referred to in paragraph 1, they shall also make such evidence*

available to requesting competent authorities from other Member States in an electronic format that allows automated exchange".

Finally, one thing certain: an important preexisting condition for proper SDG and OOP implementation is the existence of the eIDAS Regulation, to both regulate the recognition of national means of electronic identification by public authorities in cross border transactions, and to provide a legal framework for electronic signatures and electronic seals that may be used to authenticate evidences. However, there are several challenges on this point. The SDGR does not contain a requirement to use means of electronic identification which are subject to the terms of the eIDAS Regulation. Member States can take measures in accordance with EU law *"to safeguard cybersecurity and to prevent identity fraud or other forms of fraud"*. However, this is more an encouragement than an obligation. Even if all Member States would have a notified eID with high level of assurance, it would still not comprehensively resolve all challenges for identifying users. In reasoning on how address this problem, one should also take into account the potential multitude and variety of participants in an evidence exchange under the SDGR. Currently, it is largely a question of the extent to which competent authorities are willing to trust each other's procedures for the identification of users. In order to ensure additional safeguards with the possible choices (which are also political), changes will need to be introduced by the implementing acts.

4 Discussion

The empirical research based on the DE4A survey and supported by the desk research on the relevant digitalization initiatives, aimed to picture an overall level of eGovernment advancement in Europe. Attempting to cover the eGovernment blocks relevant for the DE4A project, the survey followed five major domains – Electronic Identification, Authentication and Trust Services; EU Digital Identity Wallets; Digital Service Infrastructures; Single Digital Gateway; and Once-Only Principle – which are of primary relevance for the DE4A pilots. Based on the analysis, the following remarks should be considered:

- **Progress of the state of implementation**. In line with the attempts of the European Commission to frame an implementation strategy that standardizes and guides digital transformation in Europe, most of the European countries demonstrate advancement in the state of eGovernment service implementation and availability. Although Member States demonstrate different levels of maturity and compliance with the harmonized EU level legislation, there are significant effort towards harmonization in both legislative and technological manner. As seen on the examples of the eIDAS, DSIs, the OOP and SDG implementation, the responding countries employ different legal strategies when transposing the EU legislations into their national laws. While certain countries establish tailored national policies and legislation in order to support country-wide implementation of eGovernment services (e.g. by favoring qualified or advanced trust services), others choose to rely on eIDAS as it is, without complementary national legal initiatives, or prefer to commence with the technical and operational development of supporting infrastructure without adopting dedicated national legislation. Similarly, the legal approach differs from one country to another, with some preferring the introduction of specific obligations, and others exhibiting greater flexibility. As discussed under the SDG regulation, most of the countries are highly oriented toward user-centricity, with national practices being more advanced than cross-border ones.
- **Involvement of private sector in the provision of public services.** Trust toward the role of private entities in the provision of access to public services has been also on the rise, although differently exhibited in different countries. The private sector is increasingly seen as public partner in the context of e-service provision, resulting in a higher percent of public-private partnerships (in 67% of the countries), and covering a significant share of the service market. In addition, with the revision of the eIDAS Regulation, the private sector is also directly included in the requirements for the establishment of the common Toolbox for the technical architecture, standards and guidelines for best practices. Finally, as the revised eIDAS has not entered into force yet, the private sector is the leading factor in providing a transitional model for the European Digital Identity Wallet, offering mobile solutions that work towards infrastructural migration for the upcoming changes.
- **Implementation levels affected by regulatory interdependencies.** The analysis on OOP and SDG show advancements for most of the indicators, although slower progress compared to the required level by the SDGR. Especially in aspects related to evidence exchange, procedure availability, and data protection, it becomes apparent that an important preexisting condition for proper SDG and OOP implementation is the existence of the eIDAS Regulation. It is essential to both regulate the recognition of national means of electronic identification by public authorities in cross border transactions, and to provide a legal framework for electronic signatures and electronic seals that may be used to authenticate evidences.

Although the study generally shows high progress of implementation of digital services, the results are still scattered. Despite the available common digitalization strategy and principles of the EU, certain countries demonstrate disproportionally higher level of involvement in European eGovernment initiatives than others, in addition to the with various approached in the national digitalization practices.

With all of the countries stating to have a national eID-scheme, 83% have already been (pre-)notified under the eIDAS network, being assigned to a respective level of assurance. Notably, eID schemes operated by the public sector are more broadly distributed, whereas private sector operated schemes are more broadly activated.

Requiring that all EU Member States mutually recognize national eID schemes of other countries, the eIDAS regulation obliges national eIDAS-Nodes to accept foreign eID-schemes in the national context. The report has shown that the acceptance of foreign eIDs by national eIDAS-Nodes reaches 88%, whereas the support of sending national eIDs to foreign eIDAS-Nodes is implemented in only 75% of the responding countries.

Trust services demonstrate a rather advanced development, especially the eSignature trust services. While there is no apparent evidence on any dependency of a more complex development stage of trust services (e.g. qualified trust service or advanced trust service), all three types of trust services deem to have been widely spread for national use and crossing the border for international use.

Digital Service Infrastructures, being one of the underlying elements behind European interoperability, have shown different implementation levels and (re)use by the Member States. European Blockchain Services Infrastructure, constituting an independent building block, suggests the implementation of blockchain technologies into other building blocks to increase transparency and accountability. The developed blockchain-based solutions are argued to provide more possibilities for cross-border cooperation for provision of public services. Through consolations and semi structured interviews with project partners, 13 Building Blocks and common components were found to be relevant for DE4A purposes.

Finally, essential life events, elaborated by the Single Digital Gateway Regulation, have become a baseline for the provision of public services, composing the most urgent services to be implemented in the first place. Overall, countries have demonstrated uneven level of development of the services, showing a distinctively more advanced level of implementation of the services associated with tax declaration. Equally, the SDGR procedures show various level of implementation and digitalization across countries. Some of the services that are directly involved in the development of the DE4A pilot cases show visible progress, although still low levels of implementation. This is especially visible in the context of eID-authentication and reuse of available data. The reuse of data in the context of these services is similarly limited to around 50%, leaving significant space for improvement. The mobile accessibility of the associated services is considerably high, offering mobile-enabled solutions in 80% of the cases.

Several countries with a federated structure have consistently emphasized the autonomy of regional and local governments to develop their proper eGovernment solutions. Depending on the level of legislative freedom of the subnational governments, this may entail sufficient level of liberty for carrying out subnational digitalization initiatives, which, as a result, may impact the accountability and transparency levels of public service provision.

5 Conclusions

The aim of this study was to provide an update of the state of eGovernment across European countries, focusing on the domains of electronic identification and trust services, Digital Service Infrastructures and the Single Digital Gateway. Framed by the DE4A Grant Agreement number 870635 and by additional literature research, the analysis on the eGovernment landscape mainly consisted of four parts: compliance with the regulation on Electronic Identification and Trust Services, including the revised eIDAS and the EU Digital Identity Wallets, adoption of the Digital Service Infrastructures, stocktaking of the implementation of the life events under the Single Digital Gateway, and realization of the Once-Only Principle (the full report on OOP is the subject of D1.4 deliverable "Updated Member State Once Only and data strategy Baseline").

Due to the complexity of the eGovernment concept, the research was consolidated around the most essential performance indicators identified per each domain. Both the multifaceted nature of the study and the broad set of countries with different experience in eGovernment that have participated in the survey, should have created a representative image of the current digital development in Europe. Providing a top-level overview of the status of digital initiatives in Europe, it is worth mentioning the dynamic nature of the research matter. The vast number of on-going eGovernment projects continuously shape the eGovernment landscape, reasoning the necessity for more frequent update of the established baseline. Despite the dynamic picture, a snapshot of the current level of digital integration of the European shared digital space is practical for evaluating national eGovernment strategies. The present study, measuring the advancement of the eGovernment achievements in Europe, establishes a benchmark for future digitalization initiatives, serving as a referential point for further assessments.

It is crucial, however, to recognize the importance of the national context of digitalization strategies. Despite functioning in a shared European space, all countries have different processes and legislation in place, which poses significant challenges for establishment of a seamless cross-border platform for public service provision. Furthermore, there is a common trend for increasing private sector participation in the domain of service provision, which could reorient the available services, enabling provision of non-governmental services such as telecom, banking etc. The administrative structure of the country has also been repeatedly reported as an additional factor influencing the progress of the national digitalization strategy. Finally, there are also non-decisive points in the prescription by the main regulations, that leave a wide space for amending additional change through the implementation acts, which should serve the necessary harmonization in the further digitalization efforts.

The limitations of the methodology discussed in the Section 2.3, have been addressed to the extent possible at the stage of data cleansing and data analysis, and complemented by insights from the semi structured interviews with internal and external experts. Moreover, additional data sources stemming from approaches with consistent methodologies and knowledge from the thorough desk research have been used to properly reason over the results. In addition, contextual comments by the respondents helped to further put the results into the right perspective. However, despite the measures taken to avert the risk of bias and data corruption, the study cannot be considered as completely exhaustive. The collected data in this study accounts to 63% of the respondents, leaving room for some deviations if extrapolated onto all the countries.

Nonetheless, despite the potential restrictions in the context of the result scalability, the report covers the profiles of all states participating in the subsequent pilot use cases, by this providing sufficient insight into the current level of eGovernment advancement.

References

[1] "Europe's Digital Decade: digital targets for 2030," *European Commission - European Commission*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (accessed Sep. 21, 2022).

[2] "EU: The European eGovernment Action Plan 2011-2015 - Commission Communication | Joinup." https://joinup.ec.europa.eu/collection/egovernment/document/eu-european-egovernment-action-plan-2011-2015-commission-communication (accessed Sep. 18, 2022).

[3] "Ministerial Declaration on eGovernment - the Tallinn Declaration | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration (accessed Sep. 17, 2022).

[4] *Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance.)*, vol. 295. 2018. Accessed: Sep. 14, 2022. [Online]. Available: http://data.europa.eu/eli/reg/2018/1724/oj/eng

[5] "European Digital Rights and Principles | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/policies/digital-principles (accessed Sep. 27, 2022).

[6] "eIDAS Regulation | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (accessed Sep. 17, 2022).

[7] "National Strategies - eID User Community -." https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/National+Strategies?preview=/364643428/369688618/eID_Strategies_v4.0.pdf (accessed Sep. 12, 2022).

[8] Mari Tuominen and Solène Festor, "Establishing a framework for a European digital identity | Think Tank | European Parliament." EPRS | European Parliamentary Research Service, Oct. 2021. Accessed: Sep. 11, 2022. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)694244

[9] "eGovernment Benchmark 2022 | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2022 (accessed Sep. 12, 2022).

[10] "Digital Economy and Society Index (DESI) 2022 | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (accessed Sep. 12, 2022).

[11] "A trusted and secure European e-ID - Regulation | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation (accessed Sep. 17, 2022).

[12] "A trusted and secure European e-ID - Recommendation | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-recommendation (accessed Sep. 17, 2022).

[13] "Overview of pre-notified and notified eID schemes under eIDAS - eID User Community -." https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS (accessed Sep. 27, 2022).

[14] "Future trends in electronic identification and implications for the European Commission and EU Member States - eID User Community -." https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Future+trends+in+electronic+identification+and+implications+for+the+European+Commission+and+EU+Member+States?preview=%2F78549570%2F78549713%2FTrends+report+on+electronic+identification_for+publication_v.1.1.pdf (accessed Sep. 12, 2022).

[15] Deloitte *et al.*, *Evaluation study of the Regulation no.910/2014 (eIDAS Regulation): final report*. LU: Publications Office of the European Union, 2021. Accessed: Sep. 11, 2022. [Online]. Available: https://data.europa.eu/doi/10.2759/850876

[16] "What is ebsi - EBSI -." https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi (accessed Sep. 27, 2022).
[17] "Digital Homepage." https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Homepage (accessed Sep. 27, 2022).
[18] Harold Metselaar, "D2.5 Project Start Architectures (PSA), second iteration." DE4A Project, Jul. 31, 2021. [Online]. Available: https://www.de4a.eu/_files/ugd/2844e6_062d529331194f4a8e98f9edea9e701b.pdf
[19] "About us," *Blockchain*. https://dutchblockchaincoalition.org/en/about-us (accessed Sep. 27, 2022).
[20] "SSI eIDAS Legal Report | Joinup." https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report (accessed Sep. 13, 2022).

Annex – Digital Europe for All (DE4A) survey

Digital Europe for All (DE4A) survey

Purpose of the survey and data protection

Dear member state representative,

On January 1st 2020, the EU member state-driven project Digital Europe for All (DE4A) was launched. DE4A is dedicated to creating an open and comprehensive environment and platform to support public administrations in delivering secure, high quality and fully online cross-border procedures for citizens and businesses. In addition, it will provide insights into the barriers to cross-border interoperability and the enablers for overcoming them. You can read more about the project on the project website, https://www.de4a.eu/.

The survey that we kindly ask you to fill in is a second phase of the data gathering process within the project that takes stock of the deployment of cross-border services. The results and analysis of the first phase of data gathering can be found here, under D1.x deliverables.

We will use the data collected in the second phase to analyze the implementation of specific eGovernment action points in the member states and to get insight into the progress of implementing the technical architecture and the eGovernment environment since the previous stock-taking. The derived insights and good practices will serve as practical guidelines for the development and deployment of digital public services for other EU member states, as well for self-evaluation (together with own experience) of the DE4A architecture development.

The survey consists of several blocks: (1) eIDAS National ID schemes, (2) eIDAS Nodes and trust services, (3) (European) Digital Identity Wallets, (4) Single Digital Gateway Regulation: Life Events, (5) Digital Service Infrastructures, (6) Once-Only Principle and Data strategy. Each of them aims to gather insights into the current state, the implementation process, barriers and enablers, which are to be compiled into separate reports on the elaborated topics.

We kindly ask you to provide your feedback on the current status of eGovernment in your country for each of the blocks mentioned above. With the data collected in this phase, we will compile detailed aggregated reports depicting the overall eGovernment landscape of the EU member states. We encourage you to make use of the comment boxes at the end of every subchapter of the survey in order to indicate legal, technical, or other particularities relevant for understanding the national context.

Please note that the responses obtained through the survey will not considered as the official positions of the EU Member States, and that data gathered will mainly serve to support qualitative analysis of the EU governance landscape.
No individual survey will be published in its entirety, and in case an individual response is found useful for publication, it may only be done through a consent by the responder.

Data protection statement

This survey is performed in the frame of the Digital Europe for All Project (DE4A - https://www.de4a.eu/), which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 870635.

Please note that your participation in this survey implies processing of your personal data. Personal data will be processed in compliance with the Regulation (EU) n° 2016/679 on the processing of personal data (the GDPR). The input you provide will only be shared outside of the DE4A consortium in the form of aggregated data. Within the DE4A consortium, we will process your data in order to analyse your answers as foreseen in accordance with the grant agreement, on the basis of our public interest tasks. For further information or to exercise your rights, you may contact our project DPO via privacy@de4a.eu. These rights include requesting copies, correction, or deletion of your personal data, or restricting/objecting to further processing (all within the constraints of the grant agreement). You have the right to lodge a complaint with the competent data protection authority. Do you give consent to processing the information for the purposes of this analysis under the above condition?

- ○ Yes
- ○ No

Member State Information

Please state the name of the country you are representing: _____

eIDAS: National eID-schemes

This part of the questionnaire takes stock of the implementation of national eID scheme under eIDAS Regulation (EU) No 910/2014. To fill it in, you can also consult the available information on your national eID scheme at the eID User Community.

1. Please insert below the required information regarding the status of your national eID scheme(s).

	Pre-notified	**Notified**	**Peer reviewed**
Number of eID schemes			

Remarks: _____

	Level of assurance			
	Low	Moderate	High	Not relevant / Do not know
Number of **eID schemes** with the shown level of assurance				

Remarks: _____

	Level of implementation			
	Necessary national legislation adopted	Implemented for national use only	Implemented for cross-border use	Not relevant / Do not know
Number of **notified eID** schemes with the shown level of implementation				

Remarks: _____

	Official issuer			
	Public entity	Private entity	Public-private partnership	Other
Number of eID schemes whose official issuer is:				

Remarks: _____

2. The eID scheme(s) grant(s) access to the following services (please specify the concrete sectorial services):

☐ National public services
☐ Public services by regional / local authorities
☐ Non-governmental services
☐ Private entities
☐ Do not know
☐ Other: _____

3. Please indicate possession rate for all of the notified eID schemes. (*Possessions rate is the ratio of total number of eID holders to total number of inhabitants expressed as a percentage (citizens + foreign residents).*

eID scheme (1) _____
eID scheme (2) _____
eID scheme (3) _____
eID scheme (4) _____
eID scheme (5) _____
eID scheme (6) _____

4. Please, if available indicate the activation rate for all of the **notified eID schemes** where applicable. (*Activation rate is the ratio of activated eIDs to the total number of eIDs expressed as a percentage.)*

eID scheme (1) _____
eID scheme (2) _____
eID scheme (3) _____
eID scheme (4) _____
eID scheme (5) _____
eID scheme (6) _____

5. Please indicate the use rate for the **notified eID schemes** (for cross-border use and, where available, for domestic use). (*Use rate is the ratio of eIDs which have been used at least once to access a public service to the total number of eIDs expressed as a percentage.*)

eID schemes	**Use rate**	
	Domestic use	**Cross-border use**
eID scheme (1)		
eID scheme (2)		
eID scheme (3)		
eID scheme (4)		
eID scheme (5)		
eID scheme (6)		

6. Please provide the following information, if available. If not available, mark N/A:

- Number of citizens issued with notified eID-s: _____
- Number of businesses issued with notified eID-s: _____
- Number of businesses actively using notified eID-s: _____
- Number of national online service providers accepting notified eID-s: _____
- Number of online transactions by notified eID-s (total and cross-border):
  Total: _____ Cross-border: _____

7. If there are any documented good practice experiences related to the implementation of eIDAS in your country, please provide a link/reference to the document(s).

_____
_____

8. Please provide additional information which, in your opinion, is important for the understanding of your country's context regarding the topics elaborated in this subchapter.

_____
_____
_____.

This part of the questionnaire takes stock of the implementation of national eID scheme under eIDAS Regulation (EU) No 910/2014.

eIDAS: eIDAS node and trust services

1. State the version of the eIDAS Node proxy and/or the profile supported:

_____
_____
_____.

2. Does your eIDAS-node support using your national eID(s) abroad?

○ Do not know

○ Yes

○ No (if known, please specify expected date of production): _____

If Yes, please respond to the following question:

2) As a **Sending** Member State, which countries is your eIDAS Node interoperable with to provide cross-border authentication of your national eID(s)?*

_____

3. Does your eIDAS-node support the use of foreign eIDs for services in your country?

○ Do not know

○ Yes

○ No (if known, please specify expected date of production): _____

If Yes, please respond to the following questions:

3a) How is the use of foreign eIDs enabled?

☐ Allowed only for identification and authentication in public services
☐ Possible for private sector services wihtout restriction
☐ Possible for private sector services with fee, legal or other restriction
☐ Other: _____

*3b) As a **Receiving** Member State, which countries is your eIDAS Node interoperable with to send authentication requests of foreign eIDs?*

_____

5. Please identify (mark with ***X*** the appropriate field) the advancement level of the following means/services in your country:

	Do not know	Not implemented	Necessary (national) legislative procedures adopted	Implemented for national use	Implemented for cross-border use
Electronic signature					
Advanced electronic signature					
Qualified electronic signature					
Qualified certificate for electronic signature					
Electronic seal					
Advanced electronic seal					
Qualified electronic seal					
Electronic timestamp					
Qualified electronic timestamp					
Electronic registered delivery services					
Qualified electronic registered delivery services					
Certificate for website authentication					
Qualified certificate for website authentication					
Electronic ledgers					
Qualified electronic ledgers (if available)					

6. Is there any framework or a mechanism to monitor the implementation of the Regulation in your country?

◯ Yes

◯ No

◯ Do not know

7) **If Yes**, state the purpose of the implementation, i.e. the functionality of the monitoring mechanism at a national level. Check all that applies.*

☐ To ensure implementation of the necessary changes to the relevant national systems
☐ To overview the extent to which the necessary changes have been implemented in line with the adopted measures
☐ To check whether the necessary changes to the compliance obligations by the regulated entities have been adhered to
☐ Other: _____

7. Indicate the types of barriers that the implementation of the eIDAS elements (nodes, schemes, trust services) has encountered in your country (See the provided examples below):

Legal	***Inconsistency with current legislation, hindering regulatory frameworks, inter-dependence with other regulatory acts or codes of conduct***
Organizational	***Weak or inconsistent management practices, lack of common language among organisational entities***
Technical	***Underdeveloped systems infrastructures, expert scarcity, hindering innovation***
Business	***Market disruptions, lack of market opportunities, closed business pathways***
Political	***Lack of state involvement, political frictions among state players, general political turbulences***
Human factor	***Lack of user awareness, lack of personnel training, expert reluctance to involvements***

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

8. In view of the national context, please denote (with ***X***) the level of criticality to address each of the barriers enlisted above.

Type of barrier	Not critical	Irrelevant	Can benefit from some improvements	Necessary improvements should be made	Critical to address immediately
Legal					
Organizational					
Technical					
Business					
Political					
Human factor					
Other					

9. Please provide any further information, which in your opinion is important for our understanding of your country's context about the topics mentioned in this subchapter.

_____
_____
_____.

eIDAS v2: (European) Digital Identity Wallets

Enshrined in the Revised eIDAS Regulation is a recommendation for Member States to work towards the development of a Toolbox to support the implementation of the European Digital Identity framework. The scope of the toolbox should cover all aspects of the functionality of the European Digital Identity Wallets and of the qualified trust service for attestation of attributes as proposed by the Commission's proposal for a European Digital Identity framework. As the revised eIDAS is still not enacted, the aim of this section is to inspect the current state of the Member States in terms of existing Digital Identity Wallets solutions and readiness to act towards the implementation of the revised eIDAS Regulation.

1. Are there existing Digital Identity Wallets (DIWs) at this moment in your state, when eIDAS v2 has not been adopted yet?

- ○ Yes
- ○ No
- ○ No, but it is envisaged

Other: _____

If **Yes**, proceed with answering the next questions. Otherwise, move to the next section of the questionnaire.

Please name them and provide a reference accordingly:

	Name	Reference (Link, document, etc.)
DIW (1)		
DIW (2)		
DIW (3)		
DIW (4)		
DIW (5)		

2. Who is issuer of the DIWs in your country?

	Public entity	Private entity	Public-private partnership	Other
DIW (1)				
DIW (2)				
DIW (3)				
DIW (4)				
DIW (5)				

3. (Mark all that applies) The state provides validation mechanisms for the Digital Identity Wallets:

☐ To ensure its authenticity and validity can be verified
☐ To allow relying parties to verify that the attestation of attributes are valid
☐ To allow relying parties and qualified trust service providers to verify the authenticity and validity of attributed person identification data
☐ The State does not provide such mechanisms
☐ Other: _____

4. Are there means to ensure that the DIW is free of charge to natural persons?

○ Yes
○ No
○ Do not know

5. Please provide information on the following, if available:

- Number of citizens issued with DIWs: _____
- Number of businesses issued with DIWs: _____
- Number of citizens actively using DIWs: _____
- Number of businesses actively using DIWs: _____
- Number of issued identity credentials (attestations of attributes): _____
- Number of online service providers accepting DIWs and identity credentials (attestations of attributes): _____
- Number of online transactions by DIWs (total and cross-border):
  Total: _____ Cross-border: _____
- Share of online transactions requiring strong customer identification: _____
- % of individuals doing e-commerce (ratio of users of DIW doing e-commerce vs. total number of users of DIW x 100): _____
- % of individuals accessing online public services, if available (ratio of users accessing online public services vs. total number of users of DIW x 100): _____

6. Are there accredited bodies that certify the conformance of the DIWs with the requirements laid down in the relevant paragraphs of article 6a) from the eIDAS v2?

○ Yes
○ No
○ Do not know

If **Yes**, please state how many of them are private, and how many are public:

Private: _____
Public: _____

7. Indicate the types of drivers that you see important for the implementation of the DIWs in your country:

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

8. In view of the national context, please denote (with *X*) the level of importance for each of the drivers listed above.

	FOR NATIONAL PURPOSES			**FOR CROSS-BORDER PURPOSES**		
Type of driver	***Desirable to exploit***	***Important to exploit***	***Critical to exploit***	***Desirable to exploit***	***Important to exploit***	***Critical to exploit***
Legal						
Organizational						
Technical						
Business						
Political						
Human factor						
Other						

9. Please provide any further information, which in your opinion is important for our understanding of your country's context about the topics mentioned in this subchapter.

_____
_____
_____.

1.Single Digital Gateway: Life Events

The Single Digital Gateway Regulation specifies a list of 21 procedures, covering the major life events of the EU citizens: Birth, Residence, Studying, Working, Moving, Retiring, Running a business. Please provide the current status of the digital presence and mobile availability of the 21 procedures in your country.

1. Please insert the required information on the mentioned procedures:

	Online authentication	Implementation of the OOP (data reuse)	Digitalised	Depends on procedure(s)[4]:
1.Requesting proof of registration of birth	Choose an item.	Choose an item.	Choose an item.	
2.Requesting proof of residence	Choose an item.	Choose an item.	Choose an item.	
3.Applying for a tertiary education study financing	Choose an item.	Choose an item.	Choose an item.	
4.Submitting an initial application for admission to public tertiary education institution	Choose an item.	Choose an item.	Choose an item.	
5.Requesting academic recognition of diplomas, certificates or other proof of studies or courses	Choose an item.	Choose an item.	Choose an item.	
6.Request for determination of applicable legislation in accordance with Title II of Regulation	Choose an item.	Choose an item.	Choose an item.	

[4] Denote by entering the number of the relevant procedures.

(EC) No 883/2004 (1)				
7.Notifying changes in the personal or professional circumstances of the person receiving social security benefits	Choose an item.	Choose an item.	Choose an item.	
8.Application for a European Health Insurance Card (EHIC)	Choose an item.	Choose an item.	Choose an item.	
9.Submitting an income tax declaration	Choose an item.	Choose an item.	Choose an item.	
10.Registering a change of address	Choose an item.	Choose an item.	Choose an item.	
11.Registering a motor vehicle originating from or already registered in a Member State	Choose an item.	Choose an item.	Choose an item.	
12.Obtaining stickers for the use of the national road infrastructure	Choose an item.	Choose an item.	Choose an item.	
13.Obtaining emission stickers issued by a public body or institution	Choose an item.	Choose an item.	Choose an item.	
14.Claiming pension and pre-retirement benefits from compulsory schemes	Choose an item.	Choose an item.	Choose an item.	
15.Requesting information on the data	Choose an item.	Choose an item.	Choose an item.	

related to pension from compulsory schemes				
16.Business activity: Notification, permission for exercising, changes and termination	Choose an item.	Choose an item.	Choose an item.	
17.Registration of an employer with compulsory pension and insurance schemes	Choose an item.	Choose an item.	Choose an item.	
18.Registration of employees with compulsory pension and insurance schemes	Choose an item.	Choose an item.	Choose an item.	
19.Submitting a corporate tax declaration	Choose an item.	Choose an item.	Choose an item.	
20.Notification to the social security schemes of the end of contract with an employee	Choose an item.	Choose an item.	Choose an item.	
21.Payment of social contributions for employees	Choose an item.	Choose an item.	Choose an item.	

2. Please insert the required information on the mentioned procedures:

	Mobile accessibility	**Online availability for cross border use**
Requesting proof of registration of birth	Choose an item.	Choose an item.
Requesting proof of residence	Choose an item.	Choose an item.

Applying for a tertiary education study financing	Choose an item.	Choose an item.
Submitting an initial application for admission to public tertiary education institution	Choose an item.	Choose an item.
Requesting academic recognition of diplomas, certificates or other proof of studies or courses	Choose an item.	Choose an item.
Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004 (1)	Choose an item.	Choose an item.
Notifying changes in the personal or professional circumstances of the person receiving social security benefits	Choose an item.	Choose an item.
Application for a European Health Insurance Card	Choose an item.	Choose an item.
Submitting an income tax declaration	Choose an item.	Choose an item.
Registering a change of address	Choose an item.	Choose an item.
Registering a motor vehicle originating from or already registered in a Member State	Choose an item.	Choose an item.

Obtaining stickers for the use of the national road infrastructure	Choose an item.	Choose an item.
Obtaining emission stickers issued by a public body or institution	Choose an item.	Choose an item.
Claiming pension and pre-retirement benefits from compulsory schemes	Choose an item.	Choose an item.
Requesting information on the data related to pension from compulsory schemes	Choose an item.	Choose an item.
Business activity: Notification, permission for exercising, changes and termination	Choose an item.	Choose an item.
Registration of an employer with compulsory pension and insurance schemes	Choose an item.	Choose an item.
Registration of employees with compulsory pension and insurance schemes	Choose an item.	Choose an item.
Submitting a corporate tax declaration	Choose an item.	Choose an item.
Notification to the social security schemes of the end of contract with an employee	Choose an item.	Choose an item.

Payment of social contributions for employees	Choose an item.	Choose an item.

3. What is the approximate percentage of procedures available digitally as compared to overall number of public, administrative services? (State N/A if not available)

at national level _____
at regional/local level _____
at cross-border level: _____

4. What is the approximate percentage of digital-only services (*services available exclusively online*)? (State N/A if not available)

at national level _____
at regional/local level _____
at cross-border level _____

5. Are there digital means of redress or appeal available in the event of disputes with competent authorities (as per Article 10(e) of Regulation (EU) 2018/1724)?

- ○ Yes
- ○ Yes, both at national and cross-border level
- ○ No
- ○ Do not know

If **Yes**, add a link or a reference to the service, if known: _____

6. What is the type and format of evidence to be submitted?

	Type	**Language**	**Format of the evidence**	**Origin of the evidence**
Requesting proof of registration of birth			Choose an item.	Choose an item.
Requesting proof of residence			Choose an item.	Choose an item.
Applying for a tertiary education study financing			Choose an item.	Choose an item.
Submitting an initial application			Choose an item.	Choose an item.

for admission to public tertiary education institution				
Requesting academic recognition of diplomas, certificates or other proof of studies or courses			Choose an item.	Choose an item.
Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004 (1)			Choose an item.	Choose an item.
Notifying changes in the personal or professional circumstances of the person receiving social security benefits			Choose an item.	Choose an item.
Application for a European Health Insurance Card			Choose an item.	Choose an item.
Submitting an income tax declaration			Choose an item.	Choose an item.
Registering a change of address			Choose an item.	Choose an item.
Registering a motor vehicle originating from or already registered in a Member State			Choose an item.	Choose an item.

Obtaining stickers for the use of the national road infrastructure			Choose an item.	Choose an item.
Obtaining emission stickers issued by a public body or institution			Choose an item.	Choose an item.
Claiming pension and pre-retirement benefits from compulsory schemes			Choose an item.	Choose an item.
Requesting information on the data related to pension from compulsory schemes			Choose an item.	Choose an item.
Business activity: Notification, permission for exercising, changes and termination			Choose an item.	Choose an item.
Registration of an employer with compulsory pension and insurance schemes			Choose an item.	Choose an item.
Registration of employees with compulsory pension and insurance schemes			Choose an item.	Choose an item.
Submitting a corporate tax declaration			Choose an item.	Choose an item.

Notification to the social security schemes of the end of contract with an employee			Choose an item.	Choose an item.
Payment of social contributions for employees			Choose an item.	Choose an item.

7. Can the procedures be carried out in other (than the MS national) language(s)?

○ Yes

○ No

○ Do not know

If Yes, please state in which language(s):

_____

_____

8. Are there applicable fees for carrying out any of the 21 procedures?

○ Yes (provide info): _____

○ No

○ Do not know

9. What online methods for national use canbe employed to pay the applicable fee?

☐ National banking solution
☐ Paypal
☐ Credit/debit card
☐ Do not know
☐ Other: _____

9. What online methods for cross-border use can be employed to pay the applicable fee?

☐ National banking solution
☐ Paypal
☐ Credit/debit card
☐ Do not know
☐ Other: _____

10. Does your MS make use of the Internal Market Information System (IMI), established by Regulation (EU) No 1024/2012? [for the purposes of notification and explanation of why physical presence might be required for the "fully-online" procedural steps (Article 6(4)) and for the **Verification of evidence between Member States** (Article 15)].

- ○ Yes, only for the purposes of notification and explanation of why physical presence might be required for the "fully-online" procedural steps
- ○ Yes, only for the Verification of evidence between Member States
- ○ Yes, for all relevant purposes
- ○ No
- ○ Do not know

Describe any specificities if IMI is being used: _____
_____
_____

11. Indicate the types of barriers that the implementation of the SDG procedures has encountered so far in your country and explain its implications:

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

12. In view of the national context, please denote (with *X*) the level of criticality to address each of the barriers enlisted above.

Type of barrier	Not critical	Irrelevant	Can benefit from some improvements	Necessary improvements should be made	Critical to address immediately
Legal					
Organizational					
Technical					
Business					
Political					
Human factor					
Other					

13. Please provide any further information, which in your opinion is important for our understanding of your country's context concerning the topics mentioned in this subchapter.

_____
_____
_____.

Digital Service Infrastructures

The aim of this subchapter is to identify the advancement of Digital Service Infrastructures (DSIs). The DE4A project will be implemented in compliance with the existing DSIs, with the goal of delivering a network of public services available for citizens, businesses and public administrations.

1. Do you already have an eDelivery infrastructure set up in your MS?

- ○ Yes
- ○ No
- ◉ Do not know

Other: _____

3. How many eDelivery Gateways do you foresee to use for the SDG and Once-Only Technical System?

- ○ One
- ○ More
- ○ Do not know

Other: _____

4. Which type of gateway will you use for the SDG?

- ○ Domibus
- ○ Holodeck
- ○ Do not know
- ○ Not decided yet

Other: _____

5. Does your country participate in some of the European Blockchain Services Infrastructure (EBSI), H2020, CEF Digital or Recovery and Resilience Fund projects' use cases?

- ○ Yes
- ○ No
- ○ Do not know

Other: _____

If **Yes**, please indicate the name, status (planned, implemented, in production) and operational context (e.g. public procurement, internal financial audit etc.) of each of the use cases:

Name of use case	Status	Operational context

Other remarks: _____

6. Briefly explain the types of barriers that the implementation of the DSIs and the subservices have encountered in your country:

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

7. In view of the national context, please denote (with *X*) the level of criticality to address each of the barriers enlisted above.

Type of barrier	Not critical	Irrelevant	Can benefit from some improvements	Necessary improvements should be made	Critical to address immediately
Legal					
Organizational					
Technical					
Business					
Political					
Human factor					
Other					

5. Please provide any further information, which in your opinion is important for our understanding of your country's context with regards to the topics mentioned in this subchapter.

_____
_____

Once-Only Principle and Data strategy

This part of the questionnaire inquires about the member states' implementation of the Once-Only Principle (OOP) and reuse of data principle. The OOP envisages reduction of administrative burdens for the EU citizens, businesses, institutions and public administrations by allowing them to provide a certain type of information once and implying the reuse of the collected data upon the consent of all parties.

1. Is there any national digital transformation strategy to push forth a set of strategic and tactical measures to support eGovernment development?

○ No

○ Do not know

○ Yes (please provide a link/reference to any relevant documentation):

_____

2. To what extent has your country adopted a national data strategy? Check all that apply.

☐ A strategy of reusing public sector data in the public sector
☐ A strategy for harmonization of data across selected registries
☐ A strategy for Open Data
☐ Implementation of Open Data by default
☐ One or more national catalogues of datasets to make data findable
☐ A national governance implementation supporting data access
☐ Other (please specify): _____

3. Which base registries implemented for national use can be accessed by private legal entities?

☐ Persons/citizens
☐ Vehicle
☐ Tax
☐ Businesses
☐ Addresses
☐ Building and housing
☐ Cadasters
☐ Geographical data
☐ Higher Education
☐ None
☐ Other (please specify) _____

4. What types of private companies can access base registries?

For personal data: _____
For non-personal data: _____

5. What are the access conditions?

_____

6. Please, indicate how the access to base registries is implemented. Check all that applies.

☐ Replication of registries to authorities that need access
☐ Data lookup supported by APIs
☐ Subscription of data for public services
☐ Access to base registries is subject to transactional fees
☐ Access to data services under authorization processes
☐ Other (please specify) _____

7. From the drop-down menu below, denote if there are any fees introduced for access to cross-border registries.

	Public organizations	**Private organizations**	**Citizens**
Fees for national transactions	Choose an item.	Choose an item.	Choose an item.
Fees for cross-border transactions	Choose an item.	Choose an item.	Choose an item.

Other (please specify) _____

8. What communication patterns are supported in the offering of public services in your country?

○ Synchronous (direct response to a request, typically within seconds)
○ Asynchronous (delayed response, hours or even days)
○ A mix of both
○ Do not know
Other: _____

9. Please check (with *X*) the types of personal information citizens can examine and verify the access to by public officials:

	Not implemented	Citizens can access their own data	Citizens can change (request a	Citizens can verify access to	Not applicable in my country	Do not know

			change of) their data	their data by others		
Personal file						
Tax declarations						
Medical file						
Cadasters (private property)						
Personal mandates						
None						

Other (please specify) _____

10. Mark (with *X*) the base registries for the relevant procedural requirements or preconditions for an exchange under the respective legislation:

	Persons/ Citizens	Vehicle	Tax	Businesses	Addresses	Building and housing	Cadasters	Geographical data	Higher Education	Other
No conditions[5]										
Prior request from the user										
Authorization must be written into the law										
Authorization must be obtained from an authority designated in the law										
Agreement between the sending and the receiving										

[5] Any party may receive and use our data as-is without restrictions or prior authentication (data is shared as open data)

administrations										
Obligation to use certain data formats										
Obligation for certain intermediary authorities to organise the exchanges										
Obligation to use certain security measures in relation to the data										
Limitations on the permitted use of the data										
Identity matching										
Record matching										

Other (please specify) _____

11. To what extent is OOP implemented in your country? Check all that applies.

- ○ Broadly at national level
- ○ In certain areas or organisations at national level
- ○ Broadly at regional level
- ○ In certain areas or organisations at national level
- ○ At all levels of power
- ○ Not implemented at all
- ○ Do not know

Other (please specify): _____

12. In what cross-border OOP initiatives is/has your country been involved? (E.g. TOOP, BRIS, SCOOP4C, ECRIS, CEF, SPOCS, ISA2, DE4A, etc.)

_____
_____

13. Do current national laws allow direct data exchange with a public administration from another Member State?

- ○ Yes
- ○ No
- ○ Do not know

If **Yes**, please provide answers to the following:

13a) Can this exchange happen directly based on the request from the foreign public administration without additional interaction with the user from the authority providing the evidence?

- ○ Yes
- ○ No
- ○ Do not know

13b) Is there a legal distinction between requests coming from public administrations in your own country as opposed to such from other countries?

- ○ Yes
- ○ No
- ○ Do not know

14. What other sources of OOP regulation exist in your country? Check all that apply.

☐ None
☐ Non-legislative measures (strategies, green / white papers, etc.)
☐ Written guidelines or recommendations
☐ OOP is an unwritten rule / practice
☐ Other (please specify): _____

15. How would you evaluate the general attitude and willingness in your country towards the following aspects of OOP?

	Public organizations	Private organizations	Citizens
Sharing data with public	Choose an item.	Choose an item.	Choose an item.

organizations within the country			
Sharing data with private organizations within the country	Choose an item.	Choose an item.	Choose an item.
Sharing data with other countries	Choose an item.	Choose an item.	Choose an item.
Sharing personal data with public organizations in the country	Choose an item.	Choose an item.	Choose an item.
Sharing personal data with private organizations in the country	Choose an item.	Choose an item.	Choose an item.
Sharing personal data with other countries	Choose an item.	Choose an item.	Choose an item.
Changing existing organizational processes, procedures and structures to enable OOP nationally	Choose an item.	Choose an item.	Choose an item.
Changing existing organizational processes, procedures and structures to enable cross-border OOP	Choose an item.	Choose an item.	Choose an item.
Changing existing technological solutions (information systems, architectures), etc. to enable	Choose an item.	Choose an item.	Choose an item.

OOP nationally			
Changing existing technological solutions (information systems, architectures), etc. to enable cross-border OOP	Choose an item.	Choose an item.	Choose an item.

16. How concerned are you with the effort and financial costs of adapting or implementing the following national parts of the OOP Technical System (mark the relevant choice with *X*):

	Not relevant	Very concerned	Somewhat concerned	Not concerned
eDelivery infrastructure				
Adaptation of procedures				
Adaptation of data sources				
Data service directory				
Semantic repository				
Evidence broker				
Auditing components				
Preview components				
Other:				

17. Please specify and assess the beneficial outcomes that have been observed so far for the national and the cross-border implementation of OOP.

	National implementation	Cross-border implementation
Increased efficiency	Choose an item.	Choose an item.
Administrative simplification	Choose an item.	Choose an item.
Automation of practices and processes	Choose an item.	Choose an item.
Time savings	Choose an item.	Choose an item.

Cost savings	Choose an item.	Choose an item.
Increased collaboration between agencies	Choose an item.	Choose an item.
Better governance	Choose an item.	Choose an item.
Avoidance of task duplication	Choose an item.	Choose an item.
Better data quality and reliability	Choose an item.	Choose an item.
Improved interoperability	Choose an item.	Choose an item.
Increased transparency and accountability	Choose an item.	Choose an item.
Fraud reduction	Choose an item.	Choose an item.
Increased digitalization and digitization	Choose an item.	Choose an item.

Other (please specify) _____

18. Indicate the types of barriers that the implementation of the OOP system and the data strategy have encountered in your country:

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

19. In view of the national context, please denote (with *X*) the level of criticality to address each of the barriers enlisted above.

Type of barrier	Not critical	Irrelevant	Can benefit from some improvements	Necessary improvements should be made	Critical to address immediately
Legal					
Organizational					

Technical					
Business					
Political					
Human factor					
Other					

20. Please provide any further information which, in your opinion, is important for our understanding of your country's context with regards to the topics mentioned in this subchapter.

_____
_____.

Contact information

Please provide contact details of people (name, email and/or phone number) who we could contact in case we would need some additional clarification or for the purpose of a personal interview:

_____
_____.