D1.1

Survey of related work

Project number:	959072
Project acronym:	mGov4EU
Project title:	Mobile Cross-Border Government Services for Europe
Start date of the project:	1st January, 2021
Duration:	36 months
Programme / Topic:	H2020-SC6-GOVERNANCE-2020, Governance for the future

Deliverable type:	Report
Deliverable reference number:	DT-GOVERNANCE-05-959072 / D1.1 / V1.0
Work package contributing to the deliverable:	WP1
Due date:	March 2021 – M03
Actual submission date:	31st March 2021

Responsible organisation:	TEC
Editor:	Lisa Burgstaller
Dissemination level:	PU
Revision:	V1.0

Abstract:	This deliverable provides a survey of related work with respect to mobile eID, eDelivery, eGovernment and eGovernance.
Keywords:	eID, eIDAS, TOOP, SDG

Draft

The project mGov4EU has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 959072.

Contributors

Lisa Burgstaller (TEC)
Barbara Gaggl (TEC)
Klaus-Michael KOCH (TEC)
Herbert Leitold (A-SIT)
Peter Teufl (A-SIT Plus)
Thomas Zefferer (A-SIT Plus)
Detlef Hühnlein (ECS)
Steffen Hammer (ECS)
Andreea-Ancuta Corici (FOKUS)
Thomas Lampoltshammer (DUK)
Lucy Temple (DUK)
Gregor Eibl (DUK)
Andreas Abrahams (TUG)
Thomas Lenz (TUG)
Robert Krimmer (UTARTU)
Carsten Schmidt (UTARTU)
Stefan Dedovic (UTARTU)

Draft

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability. This document has gone through the consortium’s internal review process and is still subject to the review of the European Commission. Updates to its content may be made at a later stage.

Executive Summary

mGov4EU advances the practical use of inclusive mobile Government services in Europe. The vision of mGov4EU is to enable secure and user-friendly mobile cross-border services by identifying, developing, arranging, and testing the required technical building blocks. Building blocks produced in mGov4EU are evaluated during the project by means of several pilots and can later be used to leverage arbitrary mobile Government services.

To achieve its goals, mGov4EU focuses on two areas. On the one hand, the project addresses electronic identification in cross-border scenarios. In this regard, mGov4EU builds on previous work related to the eIDAS Regulation and the eID interoperability framework defined therein. On the other hand, mGov4EU has a strong focus on secure cross-border data exchange in mobile application scenarios. There, mGov4EU builds on results of previous activities related to the SDGR. mGov4EU will carry out research to advance those areas to mobile use and combine it to enable mobile cross-border service and applications that rely both on secure and reliable user authentication and on the secure and convenient exchange of user-related data.

From mGov4EU's objectives and from the intended approach to achieve these goals it becomes apparent that the project will not start from scratch. Instead, mGov4EU will build on previous work related to electronic identification, data exchange, and mobile government. mGov4EU will carry out original research to further advance existing solutions in these areas and combine them in new ways so that the envisioned innovative mobile cross-border services can become a reality.

Since mGov4EU builds on previous work and existing solutions, it is essential to have a solid overview of the current state of the art first. Only if this is known, it can be assured that mGov4EU does not re-invent the wheel but instead makes best use of prior knowledge, efficiently re-uses what exists and further advances it. Awareness of the current state of the art is hence a crucial prerequisite for efficiently contributing to and advancing existing cross-border eID and data-exchange solutions. D1.1 does so by means of a comprehensive survey that started with a literature review in each of the topics defined for the survey and in many cases ended with a detailed overview of existing solutions and initiatives relevant for mGov4EU.

Draft

Table of Content

Chapter 1 Introduction 1
Chapter 2 Mobile Government 2
2.1 Introduction 2
2.2 Methodology 3
2.3 Findings 4
2.3.1 Quality 5
2.3.2 Trust 5
2.3.3 Awareness 6
2.3.4 Security 6
2.3.5 Infrastructure 6
2.3.6 Attitude 7
2.3.7 Perceived value 7
2.3.8 Image 7
2.3.9 Demographics 8
2.3.10 Provision 8
2.3.11 Mobile Strengths 8
2.3.12 User Experience 9
Chapter 3 Electronic Identification (eID) 10
3.1 Scope of the eID survey 10
3.2 Methodology 10
3.3 Literature review 11
3.3.1 Identity management and electronic identities 11
3.3.2 Self-sovereign identities and mobile wallets 13
3.4 eID Frameworks 14
3.4.1 Policy frameworks 14
3.4.2 Technical frameworks 16
3.5 eID solutions 24
3.5.1 Notified eID schemes 24
3.5.2 Non-notified European eID 33
3.5.3 Beyond Europe 36
3.6 Findings of the eID survey 38
Chapter 4 Cross-border data exchange 41
4.1 Introduction and methodology 41
4.2 Policy layer of interoperability 41

Draft

4.2.1 Interoperability governance – policy layer 42
4.2.2 Integrated public services governance at the EU level 43
4.3 Legal interoperability 44
4.4 Organisational interoperability 46
4.4.1 Literature review 46
4.4.2 National approaches 48
4.4.3 National and cross-border data exchange approaches 49
4.5 Cross-border solutions 50
4.5.1 eDelivery 50
4.5.2 BRIS 51
4.5.3 EESSI 51
4.5.4 EUCARIS 52
4.5.5 OpenPeppol 52
4.5.6 TOOP Solution 52
4.6 Semantic interoperability 53
4.6.1 TOOP architecture/approach 53
4.6.2 DE4A 54
4.6.3 eHealth services 55
4.7 Technical interoperability 55
4.7.1 TOOP architecture 55
4.7.2 Identity matching 57
4.7.3 Record matching 57
4.7.4 eHealth services 58
4.8 Initiatives evaluation 59
Chapter 5 Summary and conclusion 61
Chapter 6 Bibliography 62
Annex I 76

Draft

List of Figures

Figure 1: Literature search and screening process using PRISMA flowchart (Moher et al., 2009) ... 4
Figure 2: Notified eID schemes (as of March 2021) ... 25
Figure 3: Interoperability model (European Commission, 2017) ... 41
Figure 4: eDelivery 4 step model (Joao Rodrigues Frade, 2016) ... 51
Figure 5: PEPPOL eDelivery network (OpenPEPPOL, 2021) ... 52
Figure 6: TOOP architecture building blocks (BB) (source D2.1 of TOOP Project) ... 53
Figure 7: Semantic interoperability view (source D2.1 of TOOP Project) ... 54
Figure 8: TOOP architecture ... 55
Figure 9: TOOP conceptual architecture ... 56
Figure 10: TOOP message flow ... 57
Figure 11: Basic setup for implementing eID for eHealth (European Commission, 2016) ... 58

List of Tables

Table 1: Key factors and their components ... 5
Table 2: Overview of notified eID schemes ... 30
Table 3: Evaluation matrix of the cross-border solutions ... 60
Table 4: Key factor Quality and identified components ... 76
Table 5: Key factor Provision and identified components ... 76
Table 6: Key factor Perceived Value and identified components ... 76
Table 7: Key factor Demographics and identified components ... 77
Table 8: Key factor Trust and identified components ... 77
Table 9: Key factor User Experience and identified components ... 78
Table 10: Key factor Mobile Strengths and identified components ... 79
Table 11: Key factor Infrastructure and identified components ... 80
Table 12: Key factor Image and identified components ... 80
Table 13: Key factor Attitude and identified components ... 81
Table 14: Key factor Security and identified components ... 81
Table 15: Key factor Awareness and identified components ... 81

Draft

List of Abbreviations

Abbreviation	Meaning
API	Application Programming Interface
AS	Authorization Server
BRIS	Business Registers Interconnection System
CA	Certification Authority
CAS	Central Authentication Service
DID	Decentralised Identifier
DIF	Decentralized Identity Foundation
eGovernment	Electronic Government
eID	Electronic Identification
eIDAS	Electronic IDentification, Authentication and trust Services, Regulation (EU) 910/2014
EBP	European Blockchain Partnership
EBSI	European Blockchain Service
EESSI	Electronic Exchange of Social Security Information System
EIF	European Interoperability Framework
ERDS	Electronic Registered Delivery Service
ESSIF	European self-sovereign identity framework
EU	European Union
EUCARIS	European Car and Driving Licence Information System
GAM	Government Adoption Model
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications Association
HSM	Hardware Security Module
ICT	Information and Communication Technologies
ID	Identification
IdM	Identity Management
IdP	Identity Provider
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technology
JSON	JavaScript Object Notation

Draft

Abbreviation	Meaning
LoA	Level of Assurance
mDL	Mobile Driving License
mGovernment	Mobile Government
MS	(EU) Member State
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OP	OpenID Provider
OECD	Organisation for Economic Co-operation and Development
OIDC	OpenID Connect
OTP	One-Time Password
PDA	Personal Digital Assistants
QSCD	Qualified Signature Creation Device
RP	Relying Parties
RS	Resource Server
SaaS	Software-as-a-Service
SAML	Security Assertion Markup Language
SDGR	Single Digital Gateway Regulation (EU) 2018/1724
SOA	Service-Oriented Architectures
SP	Service Provider
SSI	Self-Sovereign Identity
SSO	Single Sign-On
STS	Security Token Service
TAM	Technology Acceptance Model
TRA	Theory of Reasoned Action
UA	User Agent
UMA	User-Managed Access
UNCITRAL	United Nations Commission on International Trade Law
UTAUT	Unified Theory of Acceptance and Use of Technology
U2F	Universal 2nd factor
VC	Verifiable Credentials
XML	Extensible Markup Language

Draft

Chapter 1 Introduction

This deliverable addresses the need for a comprehensive overview of the current state of the art. It does so by surveying existing works and solutions related to the topics relevant for mGov4EU. In the mGov4EU DoA, the scope of D1.1 is defined as follows: *"This deliverable provides a survey of related work with respect to mobile eID, eDelivery, eGovernment and eGovernance."*

Work on D1.1 was carried out within T1.1, which is defined in the mGov4EU DoA as *"a survey of relevant work and specifications in the area of mobile eID, eDelivery, eGovernment and eGovernance. This survey will identify the relevant standards, specifications and related scientific work to provide a sound basis for forthcoming tasks and work packages"*, namely:

- WP2 – dealing with the design of interfaces, apps and services – for which it will provide the identified related work and requirements
- WP3 – the implementation work package – which builds on WP1 indirectly, as it relies on the design and architecture developed in WP2. This is the case also for WP4, which will validate the mGov4EU solution by means of different use cases.

Both the description of T1.1 and the description of D1.1 define the following topics to be surveyed: Mobile eID, eDelivery, eGovernment and eGovernance.

Accordingly, conducted surveys that are described in this deliverable are based on these topics. However, the scope of the survey was broadened to make sure that all topics relevant for mGov4EU are covered appropriately. The scope of the survey was extended and refined in a joint effort by all involved project partners. As a result, the following topics of interest were defined for the survey:

- **Mobile government:** This topic combines the elements eGovernment and eGovernance listed in the descriptions of Task 1.1 and D1.1, where a special focus is put on mobile aspects, as they are of special relevance for mGov4EU.
- **eID:** This topic comprises the element Mobile eID as defined for T1.1 and D1.1. The scope of the topic has been broadened to not only cover mobile eID systems but also other eID solutions not solely tailored to mobile end-user devices.
- **Cross-border data exchange:** This topic evolved from the element eDelivery as defined in the original descriptions of T1.1 and D1.1. For this topic, the scope has been broadened as well to not only consider eDelivery solutions, but also other approaches to exchange data across borders as envisioned by the SDGR.

The extended and refined scope of the survey ensures that all topics and aspects relevant for mGov4EU are sufficiently covered.

This deliverable reports on the survey that was conducted and on the key findings obtained. The document's structure is organized around the three above-mentioned topics. Accordingly, Chapter 2 reports on the state of that art of mobile government and summarizes obtained findings relevant for the project. Subsequently, Chapter 3 focuses on eID and surveys existing eID solutions, underlying technical and policy frameworks, and related scientific work. Finally, the topic of cross-border data exchange is addressed in Chapter 4, which provides a profound state-of-the-art analysis regarding legal, organizational, and technical aspects.

Relevant findings of the three analysed topics are provided directly in the respective chapter. In addition, a high-level overview of the main results obtained from the work described in this deliverable is provided in Chapter 5, which finally concludes this document.

Draft

Chapter 2 Mobile Government

2.1 Introduction

Mobile Government, or mGovernment is a subset of eGovernment. eGovernment is the use of information and communication technologies (ICTs) to improve the activities of public sector organisations. In the case of m-government, those ICTs are limited to mobile and/or wireless technologies like cellular/mobile phones, laptops and PDAs (Personal Digital Assistants) (M. Kumar & Sinha, 2007, Trimi & Sheng, 2008a). Will eGovernment as we know it now be replaced by mGovernment as the dominant mode or will mGovernment be just another access channel to public administration, was already questioned by an OECD report in 2011 (OECD & International Telecommunication Union, 2011).

By translating eGovernment services to mGovernment services, these services could become mobile-friendly, accessible anywhere, and flexible in use for citizens, businesses, officials, and government employees (Tseng et al., 2008). In addition, it promises the provision of location-based government services, time-savings, on-time information and service delivery, ease of use (Ntaliani et al., 2008) and personalized service (Wang, 2014). mGovernment reflects the various applications of mobile devices in the context of public administration. The advent of smartphones and related technologies (global positioning system, messaging, facial recognition, voice messaging, sensors, etc.) is a foundation for specific public services such as public location-based services like emergency alerts or user identification like fingerprints or near-field communication technologies (Wirtz et al., 2019). Various governments are reforming public administration to improve government services to citizens through the adoption of mGovernment, where information has primarily real-time value, such as terror alerts, traffic information and road conditions, severe weather forecasts, and the like (Blackman, 2006).

Developing new mobile services that are not accepted by users increases the dropout rate and the design and implementation effort may go to waste (Kaasinen, 2005). To avoid this, acceptance of new services and technologies should be a major concern of government institutions and mobile system developers worldwide and must be considered up front (Alqaralleh et al., 2020).

Many studies have proposed and examined various models to determine the primary determinants of adoption and implementation of information technology (IT). One of the most commonly used models in the IT acceptance literature is the Technology Acceptance Model (TAM) (Davis, 1989), which was adapted from the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1977) and was originally developed to examine technology adoption and use behaviour in the workplace context. In order to harmonize the literature associated with the acceptance of new technologies, a unified model has been proposed, namely the Unified Theory of Acceptance and Use of Technology (UTAUT). The model assumes that four core constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions) are direct determinants of behavioural intention, and that these constructs are moderated by gender, age, experience, and voluntariness of use (Venkatesh et al., 2003).

A more specific model looking on the eGovernment adoption context is the eGovernment Adoption Model (GAM) (Shareef et al., 2011), which identifies the critical factors that influence the adoption of eGovernment in different levels of service maturity. GAM is a comprehensive model that consists of fourteen constructs namely: Perceived Trust, Perceived Information Quality, Perceived Awareness, Availability of Resources, Perceived Ability to Use, Perceived Compatibility, Computer Self-Efficacy, Perceived Image, Perceived Service Response, Perceived Security, Multilingual Option, and Perceived Privacy, Perceived Uncertainty and Perceived Functional Benefit. Several studies in the literature have applied the GAM model (Almaiah et al., 2020; Shareef et al., 2011).

Despite many studies conducted by various researchers in the field of mobile-government adoption (M. Kumar & Sinha, 2007), the results of this literature review show that most focused on UTAUT

Draft

and TAM models to investigate the adoption of mobile-government services. In fact, the existing literature on mobile government has not provided a comprehensive model of mobile government adoption (Almaiah et al., 2020). There is not yet a complete understanding of mGovernment adoption in the information systems (IS) literature. Therefore, empirical research in the field of mGovernment adoption is needed (Sultana et al., 2016).

For this reason, the main research question for this study is "What are the key factors driving mobile government adoption?" with the following sub-question "Which driving components could be grouped to which key factor?"

2.2 Methodology

In order to address the previously mentioned research questions, a systematic literature review was conducted. This allows for significant contribution to knowledge development, by understanding the existing publications on a specific topic and adds value by being more than a simple sum of parts (Boell & Cecez-Kecmanovic, 2014; Webster & Watson, 2002). The five steps of the Grounded Theory method proposed by Wolfswinkel, Fortmueller and Wilderom (Wolfswinkel et al., 2013) was used as a guide for conducting the rigorous literature review. Furthermore, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Moher et al., 2009) was used to report the process.

The first step was to define the criteria for the literature search. The focus was on three main concepts of eGovernment: mobile Government, mobile eVoting, and mobile Identity. Seeking only the most current and actual publications, the timeframe determined was the last 5 years (2016-2020). Since eGovernment is a transdisciplinary concept, there was no initial discrimination of fields in the initial search.

The Second step is to conduct the search, this was carried out in February 2021 using Scopus database. Three comprehensive search strings were used containing the different analogous concepts for mobile government, mobile eID, and mobile eVoting. The search allowed for results found in article title, abstract and keywords. The results returned were 150 results for mGovernment services, 58 results for mobile ID, and 50 results for mobile Voting: a total of 258 articles.

The third step requires selecting the sample of literature. Firstly, duplicates were removed from the database (2 articles). Secondly, conference proceedings, reviews and conference abstracts were removed, with a total of 125 papers remaining: peer-reviewed articles and relevant journals. All these article titles and abstracts were screened, and those out of scope, due to belonging to a different field of study, as for example medical or anthropological studies, or not being available in English, were removed. This resulted in 71 eligible articles. Finally, only 54 papers were available, due to payment restrictions and accessibility, therefore downloaded and analysed. Figure 1 details the literature search and selection using the PRISMA flowchart (Moher et al., 2009).

The fourth step was to identify according to the literature what were the components that drive mobile government adoption. A manual qualitative coding system of labelling and extracting factors affecting the adoption of mobile government took place and a total of 86 concepts were identified throughout the studies. Nevertheless, 14 studies did not show any relevant factors, therefore these were not included in the final analysis.

Finally, the fifth step grouped these concepts into the identified key factors, quality, trust, awareness, security, mobile strengths, user experience factors, demographic factors as moderating factors, service provision, image, available infrastructure, attitude, and perceived value of the service. The findings are synthesized in Annex I, and the key factors are described in the following sub-chapter.

Draft

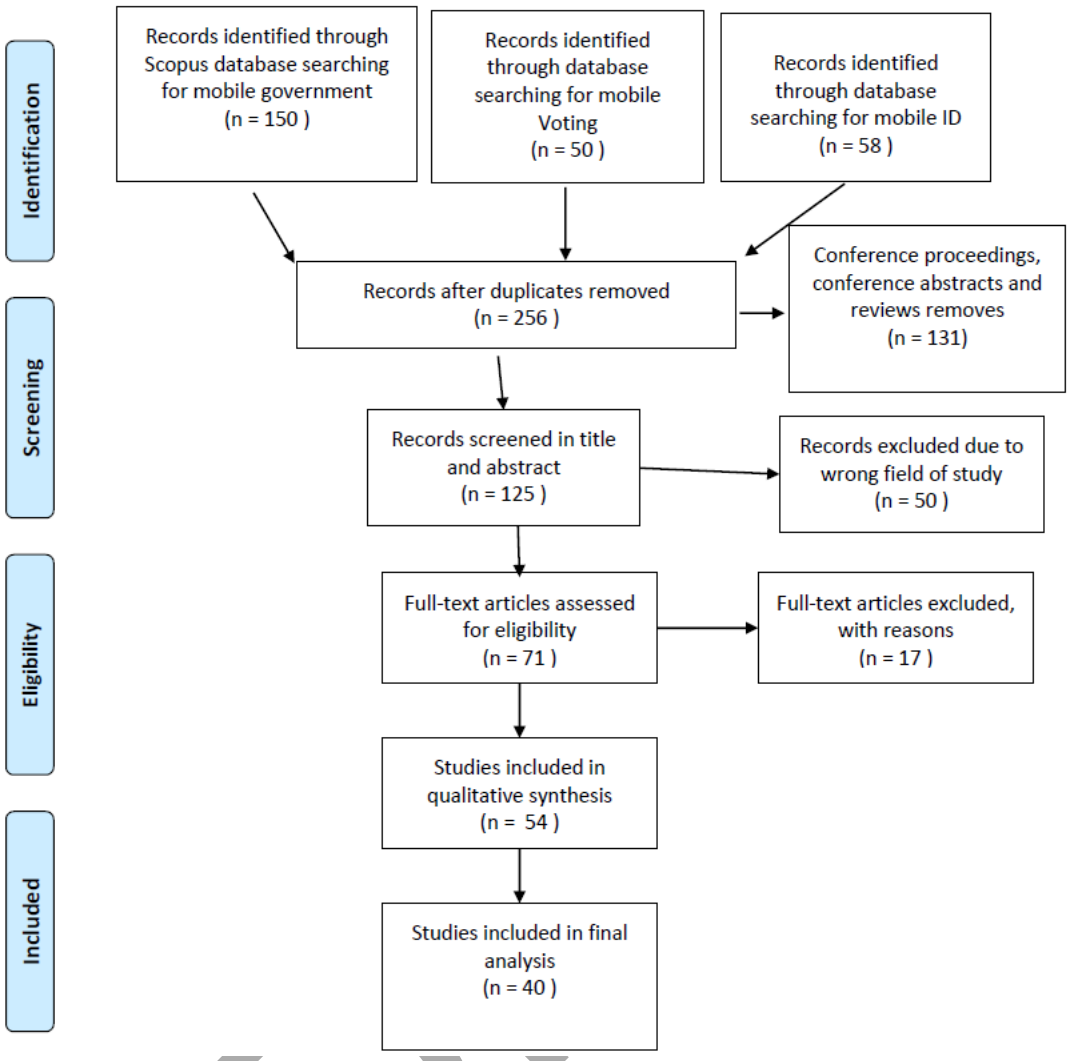

Figure 1: Literature search and screening process using PRISMA flowchart (Moher et al., 2009)

2.3 Findings

From the 86 components identified in the literature, 12 key factors were consolidated (Table 1), these are described in the following sub-chapters. The detailed components within each factor and the references that mention these components are detailed in Annex I.

Table 1: Key factors and their components

Key Factors	# of mentioned components	# of References these are Present in
Quality	7	16
Trust	7	21
Awareness	2	7
Security	3	15
Mobile Strengths	17	22
User Experience	16	26
Demographics	8	8
Provision	4	5
Image	5	6
Infrastructure	5	11
Attitude	3	4
Perceived Value	9	13

2.3.1 Quality

According to (Al-Hubaishi et al., 2018), service quality can be perceived, not as a single dimensional factor, but as a multi-faceted factor. The main components aggregated here are interaction, environment, information, system, network, and outcome-oriented quality aspects. (Chanana et al., 2016) went event one step further and split the factor into different service quality parameters, for example, protection of personal information, ease of use of application, security of financial transactions, or transparency within the actions of the application. In this context, information quality has shown not to increase the perceived usefulness of services, however, it increases the perceived ease of use (AlBar & A., 2018).

When it comes to the stability of the service, factors such as service recovery have demonstrated a positive influence towards the overall loyalty of the users towards the service (Almarashdeh, 2020) and within the same context, reliability strongly influence gratification of users (Alharbi et al., 2020). Besides these two aspects, also the ubiquity of the service play an important role for the citizens to access the service virtually everywhere and anytime (Camilleri, 2019).

Finally, there is also the accuracy of information. Studies have shown that the inclusion of multimedia content, such as video or supplementary audio can greatly support the understanding of the conveyed information and thus contribute to the overall user satisfaction (Z.-J. Chen et al., 2016).

2.3.2 Trust

Trust, or better to say, perceived trust represents a strong influential factor when it comes to influence user intention concerning the usage of a given service (Almarashdeh & Alsmadi, 2017). This holds especially true concerning trust towards mobile government solutions, as users are exposed to potential privacy and security risk during data transmission (S. Z. Ahmad & Khalid, 2017); which might not always be voluntary but demanded by law, for example. Thus, an increased level of trust does not only lead to a higher user acceptance (Alqaralleh et al., 2020), but also contributions towards the overall loyalty of citizens towards governmental services (Almarashdeh, 2020). One factor to foster trust hence is transparency, for instance, in form of access to information (e.g., in form of documents) about actions and decision taken by the government (Mishra & Singh, 2019) concerning affected stakeholder (Z.-J. Chen et al., 2016). In this context, also the information itself,

Draft

which is distributed through the governmental service should be current and reliable (Z.-J. Chen et al., 2016).

In the area of perceived risk in the context of trust, (Almarashdeh, 2020) report a tight coupling with the aspect of service quality, namely, as the level of perceived quality goes up, the level of perceived risk goes down. The authors also show that perceived risk is heavily based on behavioural and environmental influences. For example, malicious actions of service providers, e.g., concerning the provided user data, or limited service availability due to limited or negatively impacted internet/infrastructure accessibility.

Considering the impact of perceived reliability, (Shareef et al., 2016) demonstrated the importance of the overall trustworthiness of governmental applications, especially towards proper functionality and assured outcomes as announced by the service provider. What is particularly interesting is that the authors found strong indication for the different strength of this impact, depending on the cultural background of the users.

Another facet of trust can be found in procedural fairness, i.e., fairness in the context of transactions (e.g., online transaction in mobile government services). (Z.-J. Chen et al., 2016) reported that perceived fairness overall increases the level of user satisfaction. In addition, timely (time critical) responses, as well as increased precision of services via, e.g., positional data support procedural fairness. In addition, the possibility to provide own input by users (e.g., citizens) can further increase the overall level of procedural fairness.

2.3.3 Awareness

The factor of awareness has been identified as fundamental pre-condition, alongside other factors, that need to be in place for any mobile service to succeed (Al-dalahmeh et al., 2018). This has been confirmed by (Shahzad et al., 2020), who showed a significant, positively driving relationship between the awareness of citizens towards existing mobile government solutions and the intention to actually use it. The authors further stress the importance of information provision concerning the actual use-case and implementation of the mobile government service, paired with its transformational impact. Thus, strategic awareness campaigns should be considered as accompanying actions for mobile government service provisions (Mandari et al., 2017).

2.3.4 Security

The factor of security, like in other application domains as well, is one of the fundamental aspects to be considered during the development of services. (Saeb Al-Sherideh et al., 2018) agree in this regard and point out that security and privacy can be seen as critical success factors for mobile government applications. This point is further endorsed by (Onashoga et al., 2016), who argue towards the need for General Data Protection Regulation (GDPR) (or equivalent) awareness and training of government employees, as well as the adoption of privacy-by-design for mobile implementations. In addition, the authors reflect on the situation of proper policy options, which need to be present as an embedding condition.

(Eid et al., 2020) elaborated in their work how security impacts the overall acceptance of a provided mobile government service. In addition, the aspect of perceived security, i.e., the security “feeling” users have when using the service, is not to be neglected. In this context, (Ishengoma et al., 2019) also discuss the relation towards trust, as belief of non-existing or insufficient security and privacy coverage impacts the relationship between public authorities and citizens. (AlBar & A., 2018) confirm this relationship via their results pointing towards a positive effect on individual usefulness, based on the perceived security level or state of the offered service.

2.3.5 Infrastructure

Venkatesh et al. suggested that their construct "facilitating conditions" measures the degree to which individuals believe that the organizational and technical infrastructures exist to support them in using a technology system (Venkatesh et al., 2003). Existing literature has emphasized that ICT infrastructure should be stable to provide the foundations for e-government services(Ndou, 2004).

Draft

Others have shown that the most common technical barriers to the development and diffusion of m-government are the lack of reliable telecommunications and cellular infrastructure (Sareen et al., 2013).

Specifically, in the case of developing countries such as India, a well-developed ICT infrastructure is required for the successful adoption and execution of m-government (Saxena, 2018). Many developing countries have the will but not the necessary infrastructure to immediately roll out m-Government services across the country (Onashoga et al., 2016). It is argued that one of the biggest challenges to eVoting adoption in many developing countries is poor ICT infrastructure (S. Ahmad et al., 2015).

Perceived compatibility defined by Rogers (Rogers, 1995), is the degree to which an IS/IT innovation is perceived to match the needs and perceptions of potential users.

2.3.6 Attitude

Attitude plays a significant role in predicting an individual's behavioural intention to use and adopt any information system or technology in voluntary situations like mobile government and eGovernment (Saxena, 2018). Attitude describes a person's positive or negative feeling about performing the target behaviour (Davis, 1989). Typically, individuals with strong positive initiatives and characteristics are more likely to try new technologies and are expected to have positive intentions to use mobile service (Ishengoma et al., 2019).

2.3.7 Perceived value

Perceived value is the overall assessment of a user's utility based on losses and benefits that a rational decision-maker in the field of economics tends to want to maximize. This cost-benefit paradigm originated in the behavioural decision theory to explain individual choice decisions(Wang et al., 2020).

Perceived value is one of the antecedents of citizens loyalty because it decreases the need to search for different providers. Low perceived values increase the likelihood of citizen to switch vendors. It is not only money, which is valued in terms of costs, but investments like time and effort (Almarashdeh, 2020).

Compared to eGovernment, mGovernment appears to be a more cost-effective choice for users because access to mobile devices is easier, network coverage is greater, and user fees are relatively low (Trimi & Sheng, 2008). To ensure user acceptance of the price of services offered by mobile administration compared to normal office services, their value must be at reasonable prices (El-Kiki & Lawrence, 2006) and the cost of services must reflect the value of the specific services (Almarashdeh & Alsmadi, 2017).

Some technology adoption models acknowledge financial and other costs associated with using technology. The price-benefit construct has been defined in such models as the perceived trade-off between the monetary cost of the technology and the expected or experienced benefits of the technology (Venkatesh et al., 2003). However, since smartphone users can usually download and use mGovernment or city service apps at no financial cost, it appears to make more sense to focus on less tangible aspects of the cost-benefit analysis for potential users like storage space, privacy costs (Hou et al., 2020).

Based on the benefit/cost paradigm, users need to consider the perception of value at both the initial adoption and post-adoption stages (Wang et al., 2020).

2.3.8 Image

Image plays an important role in mGovernment adoption. This relates to aspects such as the relative advantage of using mobile government over other more traditional options (Mandari et al., 2017). Furthermore, this relative advantage has a positive effect on the intention of using these systems, as citizens are interested in the benefits they perceive, such as information available anywhere and anytime (Mandari et al., 2017). This image perception is tied to the idea that using mGovernment

Draft

services somehow enhances one's status and prestige in society (Mandari et al., 2017). Also, as these benefits become more visible, citizens increased awareness promotes the adoption of this technology. Therefore, governments should provide information and make citizens aware of the existing services, not only to increase transparency (Alharbi et al., 2020), but visibility is key, especially in rural areas (Mandari et al., 2017). Nevertheless, this visibility does not only respond to government promotion of the service, but also because of citizens reporting on their use to others, and the consequences of doing so, as the results are perceived to be tangible (Mandari et al., 2017).

Social Influence, as mentioned in the UTAUT model, influences citizens desire to use a service, as it relates to the perception of the opinion and beliefs that important others have on one's actions (S. Z. Ahmad & Khalid, 2017; Venkatesh et al., 2003). This is a key factor to consider, especially in small communities (Hou et al., 2020).

2.3.9 Demographics

Demographic variables such as age, gender and income have shown to have a moderating effect regarding mobile government adoption. Some studies have shown that males have an increasing tendency to adopt these services over females (Saxena, 2018). Furthermore, Saxena found that in India the age group of 31 to 40 years of age are more inclined to adopt these mobile services (Saxena, 2018).

Cities with higher poverty levels, lower levels of education, have lower mobile capacity (Mossey et al., 2019). This goes hand in hand with the need for governments to address all of their population, including the most vulnerable, making sure to be more inclusive, leaving no man behind, the progress must be felt by all the segments of society (Camilleri, 2019): this includes the technology-savvy users, the minorities and the elderly (Mossey et al., 2019). Governments should seek ways to address the digital divide and appeal to all citizens, regardless of age, income, education and gender.

2.3.10 Provision

This key factor comprehends those aspects that must be present for governments to be able to offer mobile services. Being a supportive legal and policy framework (Onashoga et al., 2016; Ryu et al., 2020; Saxena, 2018) or government support, especially in developing countries (Mandari et al., 2017). mGovernment services must be launched with a tight legal infrastructure and regulatory norms to back their implementation, citizens awareness regarding surveillance and privacy should be addressed (Saxena, 2018). Moreover, governments must shift to mobile governance, and laws and regulations should be updated to recognize and include digital transactions, and electronic documents (Onashoga et al., 2016). The service provided must address both distributive and interactional justice, citizens respond to fair and equal treatment (Almarashdeh, 2020).

2.3.11 Mobile Strengths

Mobile government, as its name entails, differentiates itself from other forms of government service due to its mobility: the opportunity to access this service at any- time, anyplace and from one's personal, portable device (Iyamu, 2020). Mobile devices are widespread and allow for governments to innovate in new ways to reach their citizens, offering new forms of delivering services, and the demand for improved government services is increasing (Almarashdeh & Alsmadi, 2017). This mobile strength allows citizens and stakeholders to access anywhere and at any moment in time, without wasting time visiting government offices, also, governments can flexibly deliver public services without a fixed location (Mishra & Singh, 2019).

The portability of this government service delivery is a convenient option for citizens(Glood et al., 2005), providing high accessibility (Ishengoma et al., 2019; Styrin & Kostyrko, 2016) and reachability. Moreover, the speed at which users can access the services has been key also for Government use, as citizens may provide emergency information, real-time information, as well as be informed of urgent situations (Lenz, 2016). The increased penetration of mobile devices over computers is also visible in developing countries; the government can reach more citizens through mobile provision of services than through traditional eGovernment (Chanana et al., 2016). Although there are many

Draft

positive aspects regarding mobile government, some authors highlight the limited computational capacity of portable devices (Iyamu, 2020; Saxena, 2018).

2.3.12 User Experience

User experience reveals those components that promote mGovernment adoption from the user or citizen perspective, some of these include the responsiveness of the system (Alharbi et al., 2020), to user satisfaction, which has a high impact, especially in developing countries with low IT development (Van et al., 2016) and the convenience of using this system over another may promote citizens to increase future use (Shahzad et al., 2020).

Technology adoption models previously described, such as TAM and UTAUT, have grasped the importance of user experience: a system's success depends greatly on the user's perspective of the benefits and ease of use. This naturally extends to the adoption of mGovernment services, many authors have empirically tested the importance of these aspects for citizens. Some of these are applying the perceived usefulness, catering to the user's needs (Saeb Al-Sherideh et al., 2018) and perceived ease of use (Eid et al., 2020), how easy a user distinguishes the system to be (Z.-J. Chen et al., 2016). Also, effort expectancy (Talukder et al., 2019), how much effort using the mobile government service will require, and performance expectancy, the extent to which the user benefits user in performing a certain task (Almaiah et al., 2020), will impact their intention to use a service.

Draft

Chapter 3 Electronic Identification (eID)

3.1 Scope of the eID survey

A main objective of mGov4EU is seamless integration of mobile cross-border eGovernment processes. This in particular involves eGovernment applications – either implemented as conventional web application ("Service provider (SP) web application"), as smartphone app ("SP app"), or as mobile eID applications ("eID app"). By focussing on the EU, the eIDAS Regulation is the main eID-related basis mGov4EU operates on. This survey, however, reached beyond to learn from other initiatives as a broader basis to build on subsequently. This broadening includes eID solutions not covered by eIDAS, like non-notified eID or emerging wallet-based solutions and self-sovereign identity (SSI) in different regions, but also international initiatives like by the UN or OECD.

Keeping eIDAS as the primary focus of mGov4EU in mind, the survey especially addresses the interfaces provided by the eID apps, which allow to recognise their presence, discover their technical capabilities and their subsequent invocation. Other aspects include a categorisation of technical choices by the eID solutions, possible dependencies like on specific devices or mobile operators, and how integration with mGovernment services can be carried out. This shall form a basis for the mGov4EU architecture to not support just solutions that are available to the mGov4EU partners, but to be flexible enough to reach beyond.

3.2 Methodology

With the aim of supporting the adjacent mGov4EU work on the architecture the eID survey shall provide a comprehensive overview of the area. This overview shall range from scientific work that gives a view on related research, via the policy environment to the technical frameworks and concrete eID implementations. These different domains - science, policy, and technology - ask for different methodologies to establish the survey.

The literature review started with a Scopus search using "mobile ID", "mobile eID", "mobile identity", "electronic identity", "identity management", "self-sovereign identity", and "decentralized identity" as keywords. With a significant amount of results, the emphasis was set on papers that indicated actual technical implementation in their abstract. This was complemented by papers known to the authors of this deliverable. This resulted in related work in two main categories, identity management and electronic identity, as well as self-sovereign identity.

To establish eID frameworks two categories were seen relevant: policy frameworks and technical frameworks like standards. For the policy frameworks, initiatives of international organisations have been summarized, namely EU, UNCITRAL and OECD, this was complemented by national initiatives. For technical frameworks, mainly standards have been listed. For both, policy frameworks and technical standards, no thorough methodology was applied, as the most relevant basis like core standards were known to the authors of the section that are experienced in the field. Still, a cross-check with surveyed scientific work and rolled-out eID solutions has been carried out to ensure that all relevant frameworks have been covered.

On actual eID implementations, a set of questions that were considered relevant for the mGov4EU implementation work has been developed. The idea was to collect a significant number of eID solutions and to analyse them systematically using the developed questions. For the actual eID solutions those notified or pre-notified under eIDAS were the logical primary focus, as these are the eIDs having a legal framework and the EU-wide recognition needed for SDGR. The notification documentation or pre-notification documentation and Web-research have been used to analyse the notified eIDs. The analysis of notified eIDs has been complemented by the description of further mobile ID solutions. The list of these additional eIDs has been established through Web-search, eID studies, and a survey.

With approximately thirty eID solutions that have been analysed against a common set of research questions, concrete findings could be established that conclude the eID survey.

Draft

3.3 Literature review

This section surveys literature related to electronic identities (eID). Focus is put on scientific publications. Furthermore, references to selected white papers are provided where appropriate. Surveyed literature is subdivided into two categories: First, scientific work related to identity management and electronic identities is surveyed in the following subsection. In the second subsection, a brief overview of relevant scientific work on self-sovereign identities (SSI) and mobile wallets is provided.

3.3.1 Identity management and electronic identities

Identity management, electronic identification (eID) and related aspects have been topics of scientific interest for years. This section gives a high-level and non-exhaustive overview of scientific contributions in respective areas focussing on those publications that are of special relevance for the scope of mGov4EU.

Identity management in general, and the application of identity-management approaches to set up national eID infrastructures has been a recurring topic in scientific publications. A rather early contribution dates back to 2012, when (Ferdous & Poet, 2012) presented a comparative analysis of popular Identity Management Systems based on different sources' requirements. A more recent survey of identity-management approaches has been provided by (Pöhn & Hommel, 2020). Their paper classifies different identity-management approaches based on a three-axis system. The system uses the topology, the type of user, and the environment to highlight the trade-off between user control and trust. The provided classification helps to choose a suitable approach to implement identity-management systems.

A comprehensive overview of identity management is also provided by (Bertino & Takahashi, 2011). In their book, the authors describe and discuss in detail core concepts, technologies, and systems of and related to identity management.

In the context of European national eID systems and with the aim to achieve interoperability between these national systems, the federation of identity-management systems has also become an emerging topic of scientific interest early. During the past years, various scientific publications have focussed on challenges that arise with the need to federate eID systems and have presented solutions to emerging problems. For instance, Lenz et al. have presented a flexible and modular identity-management architecture that focuses on federation and interoperability capabilities based on plug-able components (Lenz & Zwattendorfer, 2016a). The proposed architecture is applicable for high qualified identification systems such as national eIDs for eGovernment applications and their federation across borders.

More general overviews on the current state of implementation of the eIDAS Regulation in different EU Member States have been provided by (Mocanu et al., 2019) and also by (Roelofs, 2019). While such studies give interesting comparative insights, they usually do not analyse in detail country-specific issues that are caused by specifics of national eID systems. Country-specific challenges faced by different EU Member States during achieving interoperability between their own eID system and other foreign eID systems through the eIDAS framework have been reported by others. For instance, experiences of Slovakia with connecting their eID system to the eIDAS interoperability solution have been shared by (Andraško, 2017). Similarly, the Spanish situation has been discussed in more detail by (Rocha, 2020). Also the situation of the United Kingdom has been described in more detail by (Tsakalakisz et al., 2017).

One aspect closely related to the federation of eID systems is authorization. Already in 2013, Decat et al. discussed aspects of federated authorization for software-as-a-service (SaaS) applications (Decat et al., 2013). In their paper, the authors describe a concept of federated authorization that separates the authorization system from the SaaS application. The proposed concept is based on a middleware that centralizes authorization by using a policy-based authorization language. Even earlier, in 2008, federated authentication and authorization in service-oriented architectures (SOA) have been discussed by (Boehm et al., 2008). Authorization can also be considered a relevant topic

Draft

in the scope of federated national eID solutions. While proposed interoperability solutions for national eIDs of European countries have focused on identification and authentication, Lenz and Zwattendorfer proposed an advanced architectural design for cross-border authorization in Europe (Lenz & Zwattendorfer, 2016b). Their proposed solution extends existing cross-border eID federation implementations to bring up also cross-border authorization support into European eID infrastructures. The proposed architecture follows a modular and plug-in based approach to ease the integration into various heterogeneous eID infrastructures, which are deployed in European countries.

The topic of cross-border authorisation has also been picked up by other authors. For instance, Morgner et al. have investigated the combination of attribute-based access control architectures with the eIDAS protocols (Morgner et al., 2016). Alonso et al. also contributed to the topic of cross-border authorisation by proposing an identity framework for providing access to OAuth 2.0-based services following the concepts defined by the eIDAS Regulation (Alonso et al., 2019).

Another relevant aspect of eID federations is the exchange of user attributes between federated eID systems and challenges arising thereby. An earlier contribution to this topic has been made by Lenz in 2016 (Lenz, 2016). The author proposes a modular and flexible architecture that establishes an interoperation layer on cross-border identification and authentication attributes to meet the respective national legal and technical requirements. A more recent contribution to the topic of eID attributes has been made by Berbecaru et al. in 2019 (Berbecaru et al., 2019). Their proposal already builds on the established eIDAS interoperability layer and represents a solution to add sector-specific attributes to the eIDAS framework based on academic attributes that are exchanged between universities. In 2018, Lenz and Krnjic proposed an advanced and lightweight model for user-centric and qualified identity information that facilitates selective disclosure and domain-specific altering of single identity attributes to protect citizens' privacy (Lenz & Krnjic, 2018). This proposal addresses the problem that eID solutions only support an all-or-nothing disclosure, which implies an impossibility to selectively disclose single attributes or to rely on anonymous credentials or malleable signatures, which is not suitable for lightweight platforms.

Another direction pursued in scientific literature to meet privacy requirements during the process of provisioning attributes is the use of anonymous credentials. Underlying concepts have for instance been proposed by Brands (Brands, 2000) and by Camenisch et al. (Camenisch & Lysyanskaya, 2001). Even though computationally intensive, the approaches found its integration to commercial services, like Microsoft implementing the Brands approach under the brand "U-Prove"[1].

While security is an obvious requirement for identity-management systems, usability is another relevant factor to be considered to achieve a sufficient user acceptance. In many cases, there exists a certain trade-off between the security and the usability of a technical system, as security-improving measures typically tend to decrease usability. This can also be observed for identity-management systems. Usability-related aspects in identity-management systems are also a recurring topic in literature. For instance, Dhamija et al. have identified usability challenges in identity-management systems (together with security challenges) already in 2008 (Dhamija & Dusseault, 2008). Usability and privacy in identity-management systems have also been discussed by Jøsang et al. (Jøsang et al., 2007).

For many years, eID solutions and approaches to federate various eID systems have focused on browser-based use cases and scenarios. With the emergence and growing popularity of smartphones and other mobile end-user devices, established browser-based solutions need to be enhanced such that they can also be used in mobile scenarios. mGov4EU aims to achieve that. In several scientific contributions, challenges that might arise with new end-user devices and that must be overcome when making (federated) eID systems ready for usage on mobile devices have already been discussed. For instance, Cabaros et al. have proposed a middleware architecture that facilitates the seamless transaction of active sessions to cloud services from one end-user device to another (Cabarcos et al., 2012). Although the proposed solution rather focuses on cloud solutions

[1] https://www.microsoft.com/en-us/research/project/u-prove/

Draft

and not directly on eID systems, the tackled problem, i.e., the handling of active sessions on multiple (mobile) devices might also be relevant for the scope of mGov4EU. Also potentially relevant for mGov4EU is the agile mobile authentication process proposed by Lenz and Alber (Lenz & Alber, 2017), which closes the gap between different device and service types. The proposed authentication process uses existing functionality on mobile or smart devices to transform these devices into an authenticator for identification and authentication purposes. In 2019, Lenz and Krnjic proposed a model for a smart-device-based combination of multiple authentication-factors on mobile devices only (Lenz & Krnjic, 2019). Using this model, a user can combine various authenticators using a cryptographic protocol on the client-side only. Although this contribution discusses authentication on a generic level and does not focus solely on eID systems and their federation, aspects of the proposed model can also be useful in these specific areas and hence also for mGov4EU.

3.3.2 Self-sovereign identities and mobile wallets

Electronic identities, identity management, identity federation and aspects related to these topics have been addressed in scientific publications for many years. More recently, another research field related to electronic identities has emerged: self-sovereign identities (SSI). SSI is a new concept in identity management (IdM) and can be regarded as the next evolution step of the user-centric model with the main difference of not having to trust a central authority.

Concepts behind SSI are for instance summarized in a whitepaper compiled by Abraham (Abraham, 2017). Another overview of the SSI concept including its fundamental architecture has been provided by Mühle et al. (Mühle et al., 2018). This overview defines the essential components necessary to build an SSI system. It further details the actors of the system and discusses the essential components such as identification, authentication, verifiable claims, and attribute storage. An early introduction to the basic concepts of SSI has also been given by Allen in 2016 (Allen, 2016). This work also contains a definition of 10 principles of SSI, i.e., existence, control, access, transparency, persistence, portability, interoperability, consent, minimization, and protection. A detailed view on the concept of SSI has also been provided by Satybaldy et.al. In their work, the authors have also analysed the state-of-the-art implementations such as uPort, Sovrin, ShoCard, Civic and Blockstack. For the evaluation, the authors applied a new evaluation framework detailed in this work as well. The result shows that there exists different level of decentralization when trying to achieve SSI (Satybaldy et al., 2020).

Since SSI is still a rather new concept, there is not yet any formal definition or strict architecture, which must be followed. As a first step towards closing this gap, the Sovrin Foundation identified the following requirements of a SSI system namely governance to ensure a trust throughout the stakeholders, scalability and performance, accessibility of data and services, as well as privacy for the user (Windley & Reed, 2018).

When SSI systems are operated parallel to traditional IdM systems like governmental IdM systems, several opportunities but also further challenges arise. Creating new digital identities in a new system is a hassle for the users especially if the new identities cannot be used in all services. Abraham et al. have tackled this problem by proposing an eID derivation method that enables the combination of traditional IdM systems with SSI systems (Abraham, Hörandner, et al., 2020). This is achieved by proposing an eID derivation mechanism that allows the users to import existing eID data into the SSI system and this in a fully privacy-preserving way.

In another work by Abraham et al., the authors tackled the problem that verifying identity data, including the revocation check, in a fully offline environment was a recent problem and hindered the development of a fully digital counterpart of physical identity card like a passport or driving license (Abraham, More, et al., 2020). In their work, the authors addressed this problem and proposed a concept that allows the fully offline verification of SSIs. The solution utilizes features of the distributed ledger network to maintain a distributed revocation list and to create trusted attestations, which are verified by using a so-called trust store.

With SSI still emerging, the amount of related scientific work is still limited. However, there are several scientific publications on mobile wallets, which can be considered related to SSI, as they can

Draft

be a crucial technical building block for SSI implementations. For instance, Dai et al. proposed a Trustzone-based Secure Lightweight Wallet used for Hyperleger Fabric (TSLWHF) (Dai et al., 2021). The proposed wallet architecture defines a key, address module responsible for protecting the private keys as well as wallet's addresses in the trusted execution environment (TEE), and furthermore utilizes the same for protection of information synchronization and transaction verification. Another scientific contribution related to mobile wallets has been made by Iqbal et al. In their work, the authors tackle the problem that especially elderly are concerned when using mobile phone based wallets due to its complexity and lack of usability (Iqbal et al., 2020). To address this issue, the work discovers fingerprint verification on mobile phones especially for elderly. Based on that, a novel payment system is presented focusing on usability concerning the needs of elderly. A proof-of-concept is implemented and used for a usability test. Although not directly related to SSI, this works gives a good insight into opportunities and challenges of mobile wallets and their concrete technical implementation.

In the context of SSI, identity wallets are utilized to protect assets such as private keys, wallet addresses or identity data of the users. Ownership of identity data can be proven by being in possession of the related cryptographic key material. In contrast, the owner of the private key of a crypto wallet owns all crypto token assigned to it. Thus, the cryptographic secrets must be stored securely in a tamper resistant manner. Against this background, Soltani et al. proposed a practical key recovery model for SSI identity wallets (Soltani et al., 2019). The article first presents an evaluation of the common key recovery strategies. Next, an architecture is proposed which is used in the implementation to show the practicability and feasibility of the concept.

3.4 eID Frameworks

This section provides an overview of solution-independent frameworks related to eID. The main purpose of such frameworks is interoperability. With reference to the European Interoperability Framework (EIF), we discuss initiatives related to the four EIF layers, as follows: The EIF Legal Interoperability Layer is addressed in a sub-section on Policy Frameworks. Initiatives related to the EIF Semantic Interoperability Layer and the EIF Technical Interoperability Layer are described in a sub-section on Technical Frameworks (note, that several technical standards also address semantic aspects, which justifies combining both semantic and technical interoperability in one sub-section). The EIF Organisational Interoperability Layer addresses business process alignment which, in the context of mGov4EU, is less tied to eID as a building block, but to the overall process like SDGR-related services.

3.4.1 Policy frameworks

The Policy Framework section discusses eID-related legal frameworks. In the context of mGov4EU targeting cross-border mobile services, international initiatives are of interest. We therefore focus on such international frameworks in this section, but also give examples of non-European national initiatives to show some alternative choices states made.

3.4.1.1 eIDAS

The legal basis of mGov4EU with respect to eID and electronic signatures is the eIDAS Regulation (EU) 910/2014. Two parts are relevant for mGov4EU, the chapter on electronic identification and the chapter on trust services.

eIDAS keeps electronic identification under Member State (MS) sovereignty. Under the umbrella of a MS cooperation mechanism on interoperability and security, together with requirements for levels of assurance (LoA). Three LoAs low, substantial, and high are defined. eID means at LoA substantial and LoA high benefit from mandatory mutual recognition. eIDAS introduces the notion of "*notification of electronic identification schemes*": After pre-notification and a peer-review phase, a MS can notify its eID schemes at a certain LoA, the notifying MS assumes liability for these notified eID schemes. Other EU MSs then must recognise such LoA substantial or LoA high eIDs in their public-sector services, provided that these services also accept national eIDs. A notifying MS decides whether its eID means can also be used in other MSs' private-sector services and can set specific conditions

Draft

for private sector use. Note that we address private-sector use in the eID means overview later in this section, as setting conditions or disallowing private sector use may reduce the eID footprint services can use.

eIDAS defines a set of trust services, namely: Issuing certificates, validation services or preservation services for electronic signatures or electronic seals; electronic timestamps; electronic registered delivery services; and certificates for website authentication. A high degree of harmonisation is given for so-called qualified trust services, eIDAS lays down rules for conformity assessment, supervision, liability, and binding standards.

3.4.1.2 UNCITRAL WG IV

The United Nation Commission on International Trade Law (UNCITRAL) issued a Model Law on Electronic Signatures in 2001, shortly after the EU Signature Directive 1999/93/EC - a predecessor of eIDAS - got enacted. Like the EU Signature Directive the Model Law suggests equal treatment of hand-written signatures and electronic signatures and establishes requirements of certification service providers. A Model Law is not legislation by itself, it is meant as a blueprint states can consider when developing national laws. It still is of value as it represents a consensus view in a broad constituency. States that adopt the model law have a common legislative ground which facilitates mutual legal recognition.

Meanwhile the UNCITRAL Working Group IV on Electronic Commerce started work on electronic identity and trust services. The initiative is not yet completed, but "*Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services*" exist (UNICTRAL WG IV, 160th session, (United Nations, 2020). Like eIDAS, these provisions distinguish between eID and trust services. The eID concepts, although not identical, compare well to eIDAS. Also, the list of trust services matches eIDAS neatly, as the draft UNCITRAL provisions define electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services - all but archiving services are also given in eIDAS. While not binding for EU MS and while not yet adopted, similarities between eiDAS and UNCIRAL WG IV results can at least ease future third country agreements to mutually accept eID or trust services.

3.4.1.3 OECD

First work on eID dates to 2007 when the OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication got adopted (OECD, 2007). It was developed by the Working Party on Information Security and Privacy (WPISP) of the Committee for Information, Computer and Communications Policy (ICCP). It defines principles like a systems approach that also addresses interoperability, proportionality of the risks and responsibility of the parties in relation to the nature of a transaction, awareness of roles and responsibilities, security, and trust, as well as privacy. The Recommendation has been complemented by guidance for policy makers, like the 2011 OECD guidance "*Digital identity management for natural persons: Enabling innovation and trust in the Internet economy*" (OECD, 2011).

Meanwhile a E-Leaders Digital Identity Thematic Group has been established that discusses also decentralized identity or mobile identity. However, no publicly available report is yet available. mGov4EU will monitor the development to see if policy recommendations relevant for the project get defined.

3.4.1.4 NSTIC - IDESG

Although outdated, the National Strategy for Trusted Identities in Cyberspace (NSTIC) is discussed as an example of a government-triggered national eID initiative that - contrary to the regulative approach followed with eIDAS - called upon private sector engagement. NSTIC was an US initiative launched in 2011 by the Obama administration. It called for an identity ecosystem that shared several of the eIDAS objectives like privacy-enhancing, security, or interoperability.

The initiative consisted of pilot projects and an Identity Ecosystem Steering Group (IDESG). IDESG developed an Identity Ecosystem Framework (IDEF) that developed a functional model, functional requirements, and scoped a certification scheme. IDESG dissolved in 2018, the IDEF artefacts have

Draft

been handed over to the Kantara initiative, a trust framework providing conformance assessment in the digital identity field.

3.4.1.5 DIACC

The Digital Identification and Authentication Council of Canada (DIACC) is a further national trust framework aiming at developing a digital identity ecosystem. It is a coalition of public-sector and private-sector stakeholders. DIACC is not creating a legal basis, but by developing an interoperable pan-Canadian trust framework (PCTF) also aims at identifying need of such a legal framework.

The framework consists of components that define requirements for verification of a person, verification of an organization, or an authentication component that e.g., defines Levels of Assurance. The framework specifies processes and conformance criteria for providers.

What makes DIACC interesting in the mGov4EU context is that - even though it has been developed before decentralised identity emerged - a recent paper "*Decentralized Identity and DIACC PCTF Authentication*" discusses how such decentralized identity can be integrated with PCTF and argues that the concepts of the authentication component remain valid with this new technology (DIACC, 2021).

3.4.1.6 OSIA Initiative

The OSIA Initiative has been launched by the Secure Identity Alliance. It shall assist governments in developing national identity systems. Guiding principles are sovereignty of governments to avoid vendor lock-ins, technology neutrality, and privacy by design. OSIA consists of a set of open standards and APIs to enrol identities and to interface with government registers, namely Civil Status Registers, Population Registers, Biometrics Registers and Authentication Services, as well as Functional Registers (like voter registers, passport registers, etc.).

The set of open specification covers a functional view providing use cases (like ID request, opening a bank account, or police ID control), security and privacy specifications, and interface specifications. The interface specifications cover enrolment services, population register services, in ID usage. The ID usage, i.e., authentication using an eID, relies on OpenID Connect.

3.4.2 Technical frameworks

This section surveys technical frameworks related to eID and relevant for mGov4EU. Frameworks surveyed comprise technical solutions, protocols, and related norms, standards, and specifications. To address the main eID-related technical aspects relevant for mGov4EU, we structured the section into different subsections. Accordingly, the following subsections address the topics identity management frameworks, SSI frameworks, authentication frameworks, authorization frameworks, and initiatives specifically targeting mobile identity solutions.

3.4.2.1 Identity management

When service providers need to authenticate users (e.g., to grant or deny access to a protected resource based on predefined rules and privileges), they may engage via an identity protocol with an identity provider, which performs the actual user authentication. Generally, the user initially tries to access a protected resource at the service provider. The service provider forwards the user (and her browser) to an identity provider, which authenticates the user. Depending on the outcome of this authentication process, the identity provider issues a statement (possibly along with further user attributes) for the service provider. Given this authentication statement, the service provider can proceed to evaluate the user's authorization to access the initially requested protected resource. Various identity protocols have emerged that specify the interactions between the user, service provider and identity provider. The most important protocols and associated technical frameworks are outlined below.

3.4.2.1.1 SAML

Draft

Security Assertion Markup Language (SAML) is an XML-based framework for marshalling security and identity information and exchanging it across domain boundaries. It is primarily used to enable web-browser single sign-on (SSO). SAML 1.0 became an OASIS standard in 2002. It was substantially changed in 2005 with the introduction of SAML 2.0 (Ragouzis et al., 2008).

SAML consists of Profiles, Bindings, Protocols and Assertions. The Assertions are the holder of the security information (e.g., authentication or attribute statements) which SAML-consumers can use to make authorization decisions. Protocols define SAML-request/response pairs that embed the Assertions. These are exchanged between SAML-consumers and SAML-authorities using a communication protocol defined in SAML-bindings (e.g., HTTP). SAML-profiles are unique combinations of bindings, protocols and assertions tailored to a specific use case.

The Communication flow between the different SAML-entities using the web-browser SSO profile can briefly be described as follows. The user agent (UA) requests a secure resource at the service provider (SP), who then issues a SAML-request and redirects the UA to the IdP. The IdP authenticates the user and issues a SAML-response containing identity information. The UA forwards the response to the SP who then can base his authorization decision on the identity information provided by the IdP.

3.4.2.1.2 OpenID Connect

OpenID Connect (OIDC) is an authentication layer build on top of the OAuth 2.0 protocol (OpenID, 2021). It is supervised by the OpenID Foundation. Authorization Servers – called OpenID Provider (OP) – deliver an ID token during the authentication process. Relying parties (RPs) can use the identity information stored in the ID-token to verify the user's identity. Another addition of OIDC to the OAuth protocol is a REST-like interface that allows RPs to request basic user information. Therefore, the OP provides a UserInfo endpoint which can be accessed using the OAuth access-token.

The abstracted protocol flow is nearly the same as OAuth 2.0. The RP sends an authentication request to the resource owner, who answers with an authorization code. Using this authorization code, the RP can retrieve access- and id-tokens from the OP. The id-token (a JSON web token) holds information about the user identity and the authentication process and allows the RP to verify the user's identity. If additional information is required, the RP can send a request to the OPs UserInfo endpoint using the access token for authorization purposes.

3.4.2.1.3 eIDAS Technical Specifications

The eIDAS Technical Specifications are defined by the eIDAS Interoperability Architecture (European Commission, 2019), which is based on the Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of the eIDAS Regulation and by the documents and specifications referenced therein.

The eIDAS Technical Specifications define the technical foundation for the eIDAS interoperability framework. In particular, they specify the technical means to implement the interoperability layer for cross-border identification and authentication using national eIDs of EU MS. In its core, the eIDAS technical specification is a SAML 2.0 profile, enhanced by specifications of the cryptographic suites and of user attributes. Elements covered by the eIDAS Interoperability Architecture (European Commission, 2019) are the national eIDAS Nodes, interfaces to technical eIDAS components, details on MS selection, process flows, and metadata exchange, as well as operational and security requirements.

3.4.2.1.4 WS Federation

WS-Federation is part of the WS-* specifications (WS-Trust, WS-Security, WS-Policy, etc.) and extends WS-Trust by providing support for a federated identity management architecture. The current version of WS-Federation is 1.2, which was published in 2009 (Goodner & Nadalin, 2009).

Draft

WS-Federation relies on a Security Token Service (STS) and extends it according to identity management requirements, e.g., to make it accessible by web services as well as web browsers.

In general, WS-* or WS-Federation aim to allow the secure exchange of web service messages across different security domains or realms. The use of a web browser as a client is a special use case in the specifications, as specified in the Passive Requestor Profile. The user of realm A, who wants to access a protected resource in realm B, is redirected to the STS of the identity provider in realm A. The user authenticates at the identity provider and the STS issues a security token for realm B and thus for the resource provider. The resource provider verifies the security token and either grants or denies access to the protected resource based on the information in the token.

3.4.2.1.5 Central Authentication Service

The Central Authentication Service (CAS) was originally developed by the University of Yale and is now maintained by Apereo (Apereo, 2020). CAS depicts a SSO solution based on web technologies. Users authenticate once at a so-called CAS server (identity provider), which issues service tickets to enable access to multiple applications. To evaluate the user's authentication, the applications transmit the received service tickets directly to the CAS server, which verifies the ticket and returns appropriate user information to the service provider.

The identity protocol has been mainly defined in version 1.0 of CAS. Version 2.0 aims for proxy authentication on various levels and can be seen as an extension to version 1.0. Additionally, version 3.0 makes it possible to transmit additional identity information about the user. Both, versions 3.0 and 2.0 are fully backwards compatible to version 1.0.

3.4.2.1.6 BrowserID

BrowserID also aims to authenticate users and exchange identity information but has been abandoned (Mozilla, 2013). Mozilla introduced the BrowserID protocol for their Persona service, which is tightly integrated into the browser. Once the user has been authenticated by the identity provider's webpage, the user's browser generates a key pair and obtains a certificate from the identity provider. The browser users the key material to sign identity assertions, which can be verified by the service provider with the certificate.

3.4.2.1.7 ISO/IEC 24760:2019

ISO/IEC 24760:2019 (Information technology - Security techniques - A framework for identity management) (ISO, 2019) is relevant for any identity-management system. The standard consists of three parts. Part 1 defines general concepts of identity management. Based on that, Part 2 specifies a reference architecture and defines requirements related to the life cycle of identities. Finally, Part 3 provides best practices for the given context.

3.4.2.1.8 ISO/IEC 29003:2018

ISO/IEC 29003:2018 (Information technology - Security techniques - Identity proofing) (ISO, 2018) focuses on the aspect of identity proofing, which is a crucial aspect in most identity management systems. It is hence closely related (and applicable) to identity management systems. The standard first introduces and defines concepts related to identity proofing. This way, it gives guidelines for the identity proofing of a person and specifies levels of identity proofing. Based on these foundations, the standard then defines requirements related to identity proofing that must be met to achieve the predefined levels.

3.4.2.1.9 ETSI STF 588

STF 588 is an ETSI Specialist Task Force that focuses on Identity Proofing for Trust Service Subjects. The emphasis of this task force is hence related to identity management. According to the task force's website, "the scope of the STF mission is to produce specification on identity proofing for trust services as defined by eIDAS, in particular for issuers of qualified and non-qualified certificates supporting electronic signatures, electronic seals or website certificates. It needs to be aligned with, and to further support the ETSI EN 319 411 parts 1 and 2 providing policy requirements

Draft

for Trust Service Providers (TSP) issuing such certificates." (ETSI, 2020a). Beside this scope, results of this STF might also be relevant and applicable in eID-related areas.

Results of this task force will be incorporated into ETSI technical reports and technical specifications. Concretely, results from a conducted survey of technologies and regulatory requirements for identity proofing for trust service subjects are incorporated into ETSI TR 119 460 (Electronic Signature and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects) (ETSI, 2021, p. 460). Accordingly, input is also provided for ETSI TS 119 461 (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects) (ETSI, 2020b, p. 461).

3.4.2.1.10 NIST SP 800-63

SP 800-63 (Grassi et al., 2017) is a NIST standard on Digital Identity Guidelines. It consists of four documents addressing different aspects of digital identities. SP 800-63 Digital Identity Guidelines is the main document and gives an overview of general identity frameworks. It elaborates on using authenticators, credentials, and assertions in a digital system, and defines a risk-based process of selecting assurance levels. The main document SP 800-63 also refers to the other three documents part of this standard and described briefly below.

SP 800-63A focuses on enrolment processes and identity proofing within these processes. Accordingly, this document covers the first phase an entity needs to carry out to become enrolled within an identity system. SP 800-63B then addresses the subsequent phase and hence focuses on the authentication and lifecycle management. The document focuses on the challenge to reliably authenticate entities in subsequent sessions and to provide assurance that the entity currently accessing a service is the same as that which accessed the service in previous sessions. Finally, SP 800-63C addresses aspects related to the federation of identity systems and the exchange of identity assertions containing results of authentication processes between these federated systems.

3.4.2.2 SSI frameworks

SSI is a rather new concept. Still, several frameworks already exist that implement at least parts of the concepts defined by SSI. In the following subjection relevant SSI frameworks are briefly summarized.

3.4.2.2.1 uPort

The 2016 founded company uPort (UPort, 2021) aims to provide end users with an improved user experience on data verification, password-less authentication, and digitally signed transactions, all based on information stored on the Ethereum ledger. In the SSI community, uPort is one of the main players providing software libraries and documentation, following the general concept of SSI and related guidelines, for developers and companies that are interested in creating an SSI system or parts of it like implementing an identity wallet. One drawback of the uPort libraries is that they only work with Ehereum based identifiers, meaning that the use of these libraries will limit the implementation to Ethereum and Ethereum-based ledgers. Nevertheless, libraries provided by uPort are in an advanced development state and the software is permanently maintained and updated versions are released on a regular basis.

3.4.2.2.2 Decentralized Identity Foundation

Decentralized Identity Foundation (DIF) is a non-profit organization with 56 members forming a consortium. *"Enable a world where decentralized identity solutions allow entities to gain control over their identities and allow trusted interactions."* is the vision of DIF, stated on their website (DIF, 2020). DIF actively contributes to the development and enhancement of related standards as well as performs dissemination actions to bring their work and visions to related stakeholder and organisations. Additionally, DIF is also providing software implementations of the standards to which DIF is contributing. The standards for decentralized identifier (DID), verifiable credentials (VC), DIDcomm, DIDAuth are reflecting an excerpt of the standards to which DIF is contributing. DIF is

Draft

also researching and developing new methods related to the decentralized identity world but also permanently enhancing the state-of-the-art.

3.4.2.2.3 Hyperledger Indy

Hyperledger Indy is a project under the Hyperledger umbrella (The Linux Foundation, 2020b). Indy is a distributed ledger implementation, originally developed by Sovrin (Sovrin Foundation, 2021), but later moved to Hyperledger for further development, with the main purpose of enabling SSIs. In contrast to other ledger implementations, which are able to be used for more than one use case, Indy was specifically designed for the decentralised digital identity purpose only. Besides the ledger implementation, Indy offers also an SDK which can be utilized by developers to extend the default functionality of the ledger and further to integrate Indy into their software ecosystems. Even though the source code is stable and permanently further developed, using Indy comes with a vendor lock-in, meaning that the solution will not easily be interoperable with other types of ledgers.

3.4.2.2.4 Hyperledger Aries

Hyperledger Aries (The Linux Foundation, 2020a) is a framework which implements the so-called agent technology. Agents are used in the SSI and Blockchain world for communication. In contrast to client-server communication where the client and the server have different roles, all agents in the agent-to-agent communication assume the same role. Aries provides open-source agent implementations in different programming languages. The functionality of these agents is beside establishing a secure communication channel also the management of the cryptographic key material as well as the secure storage of the user's identity data. Besides the source code, Aries also offers RFCs specifying various protocols and interfaces. Aries was originally a part of Indy but was extracted for further reuse. The different Aries implementations are at different technology readiness level where the Python implementation can be seen as the most stable implementation with the drawback of only being able to communicate with Indy out-of-the-box. Other implementations like the Go implementation are an important contribution especially for the mobile world, but still in development, thus, not all the functionality is there yet.

3.4.2.2.5 ESSIF

The European self-sovereign identity framework (ESSIF, 2021) is part of the European Blockchain service infrastructure (EBSI, 2021). EBSI is a joint initiative of the European Block chain partnership (EBP) and the European Commission to provide EU-wide cross-border public services using blockchain technology. ESSIF allows users to create and control their own identity across borders without relying on centralized authorities by implementing a generic self-sovereign identity (SSI). The goals are to provide seamless cross-border services for citizens, help make institution more efficient and facilitate economic activity flow across borders.

ESSIF describes the roles issuer, verifier (service provider) and holder (subject). The holder is the owner of credential information which is stored on a personal repository (e.g., mobile phone or cloud). These credentials are provided by issuers and can be used to apply for services of verifiers. To manage credential information ESSIF uses decentralized identifiers (DID) which are registered on a ledger. By introducing an abstraction to its infrastructure layer ESSIF allows for integration of different block chain technologies (e.g., Hyperledger Fabric or Ethereum). Secure communication between parties relies on mutual authentication based on TLS certificates.

3.4.2.2.6 W3C Verifiable Credentials

The W3C verifiable credential (VC) data model (W3C, 2019) is a W3C recommendation from 2019. In the given context, the term "credential" refers to identity related information asserted for a specific identity. Examples for such credentials are driving licences (asserting the capability of operating a motor vehicle) or university degrees (asserting a certain degree of academic education).

The W3C verifiable credential data model defines the data format for representing such credentials. In particular, the VC specification states the mechanisms to express those credentials online such that they are cryptographically secure, that privacy is respected, and that they are machine-readable.

Draft

VCs are often used in SSI systems because of its flexible and lightweight format. This makes them a potentially relevant concept for mGov4EU too.

3.4.2.2.7 W3C Decentralized Identifiers

Decentralized Identifiers (DID) are a special type of identifiers that aim to enable verifiable and decentralized digital identities. This makes them a relevant concept for decentralized applications in general, and for mGov4EU in particular, as this project also aims at investigating wallet solutions based on Hyperledger technology.

Decentralized Identifiers (DID) are specified by the W3C working draft (W3C, 2021b) on decentralized identifiers (DID). Amongst other things, this specification defines the syntax of a DID. Essentially, a DID is an URL that associates a so-called DID subject with a so-called DID document. In other words, a DID subject is the entity identified by a DID and described by a DID document.

Any entity can be a DID subject. This includes persons, groups, physical things, organizations, etc. The general concept of DID is flexible enough so that they can be used for any type of DID subject. DID documents are used to describe a DID subject, i.e., the contain information associated with a DID. Typically, DID documents contain verification methods (e.g., cryptographic public keys), and services that are relevant with regard to interactions with the associated DID subject. In addition, a DID document also contains a set of generic properties. All concepts related to DIDs (i.e., DID subjects, DID documents) are specified in detail in the respective W3C working draft.

3.4.2.3 Authentication frameworks

This section surveys multiple protocols and frameworks that enable to integrate strong authentication mechanisms to replace password-based approaches by introducing other factors, e.g., possession of key material or a device.

3.4.2.3.1 FIDO

FIDO has been developed by the FIDO alliance with the aim to replace password-based mechanisms by making easy-to-use factors offered by modern devices, e.g., fingerprint, widely available. FIDO defines a challenge-response protocol, where the sign-key is unlocked through local authentication. Various types of local authentication can be integrated, ranging from security key (hardware token) to facial recognition, fingerprint, or voice matching, depending on the capabilities of the user's device. Two main specifications have been developed. Firstly, the universal authentication framework (UAF) (FIDO Alliance, 2020) specifies the messages and steps of the challenge-response protocol. Secondly the universal 2nd factor (U2F) (FIDO Alliance, 2017) specification aims to extend existing password-based authentication with a second authentication factor that is demonstrated via FIDO. Support for FIDO has been built into multiple platforms, such as the Windows 10 and Android operating system, and browsers including Google Chrome, Mozilla Firefox, and Microsoft Edge.

3.4.2.3.2 FIDO2

FIDO2 represents the next evolutionary step within the FIDO alliance, which builds upon W3C's WebAuthn and the Client-to-Authenticator Protocol (CTAP). W3C WebAuthn (W3C, 2021a) specifies a Javascript API for browsers to register a user for a website, trigger authentication and to return the authentication assertion. The implementation of API may integrate various authenticators, either on the device itself (e.g., in a Trusted Platform Module), or off device on roaming authenticators that are accessed via, e.g., Bluetooth Low Energy (BLE) or Near Field Communcation (NFC). The Client-to-Authenticator Protocol (CTAP) (FIDO Alliance, 2019) has been developed by the FIDO Alliance to specify the communication with such roaming authenticators. Besides an abstract API, CTAP also defines message encoding, bindings, and requirements for transport protocols (USB, NFC, Bluetooth).

Draft

3.4.2.3.3 GSMA Mobile Connect

Mobile Connect (MobileConnect, 2021) is an identity service that provides authentication, authorization and identity verification of mobile users. Mobile Connect is driven by the GSM Association (GSMA). The technical key element of Mobile Connect is the so-called Mobile Connect API, which can be used by service provider applications to call the required functionality (e.g., user authentication). The respective functionality is then provided by so-called Digital Service Providers (DSP).

Being mainly driven by the GSMA and hence by mobile network operators, users' identities are closely related to their mobile phone number. User authentication is typically based on the authentication factors possession and knowledge. Accordingly, during authentication users are required to prove possession of their mobile phone and to prove knowledge of a secret PIN. On a technical level, Mobile Connect is based on OIDC, hence following an established protocol standard.

3.4.2.3.4 ISO/IEC 29115:2013

ISO/IEC 29115:2013 (Information technology - Security techniques - Entity authentication assurance framework) (ISO, 2013) provides a framework for managing entity-authentication assurance. The standard defines four Levels of Assurance (LoA) and associates these four LoAs with requirements concerning control technologies, processes, and management activities. To be specific, the standard introduces all actors involved in an entity-authentication process first.

Overall, the standard comprises aspects on both technical and management/organizational level. Technical aspects are considered for the enrolment phase, credential-management phase, and entity authentication phase. These three phases are defined and specified by the standard in detail. For each phase, specific technical requirements are then elaborated. On management and organizational level, various aspects such as service establishment, legal and contractual compliance, financial provisions, information security management and audit, etc. are considered.

3.4.2.3.5 ISO/IEC 29191:2012

ISO/IEC 29191:2012 (Information technology - Security techniques - Requirements for partially anonymous, partially unlinkable authentication) (ISO, 2012) provides a framework and establishes requirements for partially anonymous, partially unlinkable authentication. The use cases addressed by the standard can be valuable in situation where entities to be authenticated need to stay - at least partly - anonymous and unlinkable, while re-identification at a later point in time shall still be possible (provided there are legitimate reasons).

The standard consists of a rather concise main part, which introduces a general framework and defines concrete requirements. In addition, the standard provides two informative annexes introducing relevant use cases and discussing the application of mechanisms for the purpose of data authentication and data protection.

3.4.2.4 Authorization frameworks

Authorization is a topic closely related to authentication. While authentication deals with verification of claimed identities, authorization controls access to resources based on defined rules. Often, an effective authorization mechanism necessitates a previous authentication, so that access privileges assigned to an entity can be enforced. The following subsections briefly survey some common authorization frameworks that are often applied together with authentication frameworks.

3.4.2.4.1 OAuth

OAuth is an open standard protocol for token-based authorization. It was first introduced in 2007 as OAuth 1.0 (IETF, 2007). Its complexity led to a complete rework resulting in OAuth 2.0 (IETF, 2012), which was published in 2012 in RFC 6749 and RFC 6750. OAuth 2.0 is not backward compatible and has largely replaced its predecessor. It uses time limited access- and refresh tokens to minimize the risks of a security breach.

Draft

OAuth defines the four basic roles: resource owner, resource server, authorization server and client. The resource owner is the holder of a secure resource, which is stored at the resource server. The client can be a desktop-, web- or mobile-application requesting access to the resource owners secure resources. An authorization server authenticates the resource owner and provides access- and refresh-tokens for a specific scope to the client.

The abstract protocol flow can be described as follows. A client who wants to access a secure resource sends an authorization request to the resource owner, who replies with an authorization code. The client then uses the authorization code to get a time limited access token from the authorization server. This access token can then be used by the client to access the secure resource stored at the resource server.

3.4.2.4.2 UMA

User-Managed Access (UMA) (Thomas Hardjono, 2012) has been developed by the Kantara Initiative to extend OAuth such that the server holding the user's resource and the server performing the authorization decision can be completely decoupled. UMA defines two main API at the Authorization Server (AS). The protection API formalizes the communication between the AS and the Resource Server (RS), while the authorization API specifies the interaction between the AS and the requesting client.

Initially, the RS registers resource sets of the user at the AS according to the resource set registration specification (T. Hardjono et al., 2015). Once a requesting client attempts to access resource at the RS, the RS registers a permission request at the AS and returns a permission ticket to requester. Next, the requesting client contacts the AS to obtain permission, where it supplies this permission ticket. The AS determines if the requester is allowed to access the user's resource according to the user's policy or an on-demand answer, which may require to authenticate the requester, e.g., with OpenID Connect. On success, the requester receives a requesting party token, which it provides in second attempt to access user's resource. The RS evaluates the token, possibly by calling the introspection endpoint of the AS, to assess whether it contains sufficient permissions.

3.4.2.5 Mobile apps and solutions

This section briefly surveys relevant technical frameworks that support the development of mobile solutions that require integration of eID functionality. Such frameworks are especially relevant for mGov4EU, as the project aims for the realization of mobile-only use cases that involve secure and reliable identification and authentication of users.

3.4.2.5.1 ISO/IEC FDIS 18013-5:2020

ISO/IEC FDIS 18013-5:2020 (Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application) (ISO, 2020) is the fifth part of the standard ISO/IEC 18013:2020 on ISO-compliant driving licences. While all parts of this standard address topic related to driving licences, Part 5 especially focusses on the implementation of a driving licence in association with a mobile device. Concretely, ISO/IEC FDIS 18013-5:2020 describes interface specifications for a mobile driving licence (mDL) application.

The standard defines functional and technical requirements for an mDL application first. It then specifies in detail a data model that meets these requirements. The standard also specifies necessary transaction related to mobile driving licences, putting a special focus on the retrieval of required data. Finally, the standard concludes with a rather detailed specification of security mechanisms to be applied for ensuring the security of stored data, conceived transactions, and the mDL application as a whole.

3.4.2.5.2 NIST SP 1800-13

NIST SP 1800-13 (NIST, 2019) addresses aspects related to single sign-on solutions for mobile applications. The publication comprises three volumes. Volume A contains an executive summary only. Volume B first provides an overview of the approach followed. It then presents the proposed architecture and concludes with a security characteristics analysis and future build considerations.

Draft

Finally, Volume C contains a guide demonstrating an example solution for the proposed architecture. Focussing on single sign-on in mobile applications scenarios, this NIST special publication can potentially provide useful input for mGov4EU.

3.4.2.5.3 RFC 8252

RFC 8252 (Bradley & Denniss, 2017) addresses challenges arising when using OAuth 2.0 in native mobile apps. It details security and usability aspects to be considered when applying OAuth procedures that require direct communication between multiple apps on the same mobile device. Such procedures can be of special relevance when aiming for mobile-only use cases requiring user authentication through national eID systems. Accordingly, RFC 8252 can be considered highly relevant for mGov4EU.

3.5 eID solutions

This section discusses eID solutions, both national eID and private initiatives. Given the environment mGov4EU operates in - SDGR and mobile solutions - the main focus is on eIDs that readily support this, i.e., national programmes that have been notified as eID schemes under eIDAS. The overview, however, goes beyond as on the one hand, further eIDs will get notified in the course of project. On the other hand, mGov4EU is a research project that enters uncharted waters with aiming at mobile public services that so far do not exist cross-border. We, therefore, also investigate interesting mobile eID solutions in the market. The purpose is to learn from such initiatives and to see what can be considered in the project.

We first describe all eID schemes that had been notified under eIDAS when this deliverable was produced. This does not only cover mobile eIDs, but also eID schemes tailored to more traditional desktop environments. The section continues with other European eID schemes. There, the focus is more on mobile solutions. It covers national programmes that might soon get notified, but also private-sector initiatives. We continue with some selected non-European eID solutions, again with emphasis on mobile eID. This part on eID worldwide cannot be comprehensive, but the mGov4EU consortium felt it useful to reach out broad and to survey also solutions that might complement what has been found within the European public and private programmes.

Each of the three sub-sections, i.e., notified European eID, other European eID, and selected solutions beyond Europe, is guided by a similar set of questions that the description of each eID scheme shall answer. The purpose is to get a comparable view of the state of the art. This shall assist adjacent work packages, in particular on the architecture, in their assumptions on what eID exists and what to expect in terms of how these can integrate with services.

3.5.1 Notified eID schemes

This section describes the eID schemes EU Member States (MS) had fully notified when this deliverable was produced. This landscape consists of 18 eID schemes that have been notified by 14 MS. Note that some MS, i.e., Belgium, Italy, Portugal, and The Netherlands, have notified multiple eID means in separate notification procedures. The number of different eID means is actually higher, as some MS combined technically different eIDs in one notification (e.g. Estonia and Latvia both notified their card-based and mobile eID versions within one notification procedure), other MS notified frameworks that federate between different identity providers that - within the technical boundaries of the respective framework - issue quite different credentials (e.g., the Italian SPID federation or the eHerkenning trust framework in The Netherlands). The set of currently notified eID schemes is outlined in Figure 2.

Draft

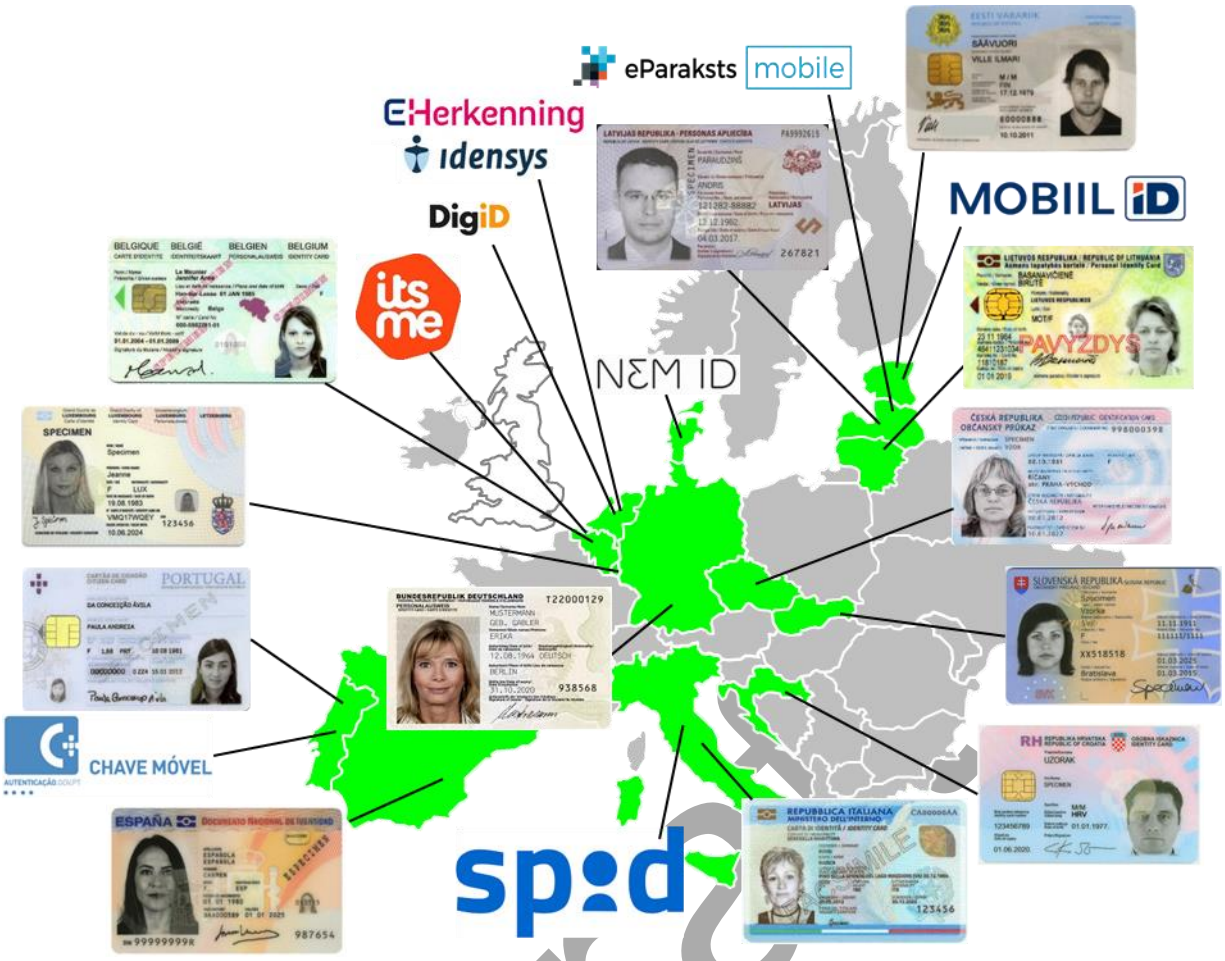

Figure 2: Notified eID schemes (as of March 2021)

In the following section we briefly describe the notified and pre-notified eID schemes in alphabetical order by MS. The descriptions aim at answering the following research questions:

- What basic technology is used by the eID scheme (card, mobile, or others)?
- What is the eIDAS Level of Assurance (LoA) supported by the eID scheme?
- Are electronic signatures supported by the credentials?
- Is it a public-sector or private-sector driven scheme?
- How is integration with relying parties done?
- Is the eID scheme limited to relying parties from the public sector, or is it open to the private sector as well?
- How can identity matching be done if identifiers are not persistent or unambiguously unique?

These questions aim at providing a solid foundation for the subsequent work in mGov4EU, like which MS already have a mobile eID or which eID schemes may provide a reasonable basis for the envisioned mGov4EU signature pilot. The short descriptions are meant to serve as a first point of reference rather than the mature result of a well-grounded in-depth technical analysis. In addition to the survey results summarized here, however, the related technical specifications have been collected so that a reference base is available to the corresponding technical work of mGov4EU.

3.5.1.1 Belgian FAS

Belgium was among the first countries introducing an eID, which was initially based on the ID card. This evolved to a federal authentication service (FAS) allowing for various authentication providers and different LoAs. The public-sector card-based "eCard" and the private-sector-driven mobile solution “its.me" got notified at eIDAS LoA high. Unique identification is based on the population register and qualified electronic signatures are supported in both cases. The QSCD is the smartcard for the eCard and a qualified remote signature service for its.me.

The integration with FAS uses SAML and, it is currently limited to public sector relying parties. This covers the identification part, the central federation platform de-couples from specifics of the different authentication credentials. The mobile its.me is integrated with public services through FAS, but its.me also allows for direct integration with private services for desktop web, mobile web and mobile app using OIDC. its.me signatures are integrated through a JSON-based Signature Creation Application Backend. Service providers are registered at the its.me service.

3.5.1.2 Croatian eID Card

The Croatian eID Scheme “National Identification and Authentication System” (NIAS) uses the Personal Identity Card (eOI) as a means of electronic identification. It is notified with the eIDAS LoA high. The eOI unique identification is based on Ministry of Interior (MUP) Registers. It also acts as a QSCD and can hence provide qualified electronic signatures.

NIAS is based on the SAML protocol and has the role of a mediator (gateway) between users, public services and identity providers in the process of applying to e-services. It is only open for integration of public-sector services. The user interaction is browser based via the E-citizens web portal.

3.5.1.3 Czech eID Card

The Czech Republic has notified its identity card as eID at LoA high. It is a contact-chip smartcard that also is a QSCD that citizens can activate for qualified electronic signatures. The eID is public-sector issued and limited to Czech citizens, unique and persistent identification is ensured through the population register.

Integration with services is SAML-based. The user gets redirected from the relying party to the National Authentication Authority (NIA) which, after selection of the eID card as authentication means, further redirects to the eID card IdP that carries out authentication through secure messaging with the card applet. The eID scheme creates relying-party-specific pseudonyms for services in the Czech Republic. This can be public sector relying parties or private parties that have an obligation to verify a user’s identity. For cross-border transactions, identifiers are derived MS-specific with different identifiers for public sector and private sector. These different identifiers need to be considered in the receiving country’s identity matching concepts.

3.5.1.4 Danish NemID

The Danish NemID has been notified at LoA substantial. The eID scheme is contracted by the Danish government, it is open to public sector and private sector services. The eID scheme consists of different credentials as drivers as username/password with printed key-cards, with one-time password (OTP) key-tokens, a mobile app using PINs or biometrics, USB tokens, or a phone call-back for interactive voice response OTP for visually impaired. The scheme does not include solutions for qualified electronic signatures.

A persistent unique identifier is based on the national identity number for residents or an administrative number for non-residents like students or commuters. For cross-border transactions a MS-specific persistent identifier is calculated. Service providers in Denmark get issued an authorisation certificate that allows joining the federation. Integration of services is through SAML or OIDC.

Denmark is working on a successor programme MitID that was planned for 2021.

3.5.1.5 Estonian ID card and Mobiil-ID

Estonia has notified six different eID schemes divided into only digital eIDs and digital eIDs with a physical representation of the identity. The two major schemes are the Estonian ID-card (smartcard) and the Mobiil-ID (simcard). Both schemes have a high LoA. The unique identification is assured by the Estonian population register and the identity documents database. The Mobiil-ID smartcard can only be issued to owners of an Estonian ID-card. Both, smartcard and simcard can be used as QSCDs for qualified electronic signatures.

Draft

The authentication process is SSL/TLS client-certificate based, so both public and private sector entities can integrate it. Certificate validity check is done via online certificate status protocol (OCSP), which requires an agreement or contract with the certification authority (CA). In case of Mobiil-ID, the validity check is done by the central service (DigiDocService). Therefore, an agreement with the central service provider is necessary.

3.5.1.6 German nPA

The "German eID based on Extended Access Control" (EAC) was the first eID scheme to be notified in 2017. It is based on the German national identity card and electronic residence permit, which are contact-less chip-cards, and has the eIDAS LoA high. The unique identification is assured by decentral registers, identifiers are service-specific and card-bound, i.e., change when the citizen replaces the ID card. Identity matching is supported by additional attributes (name at birth, place of birth, and date of birth). The identity cards would technically be capable to serve as QSCDs but would require a rather sophisticated technical infrastructure service for the installation of qualified certificates onto the chip-card, which has been deprecated by the identity document issuer in favour of an alternative solution based on the remote signing paradigm.

Due to the use of the EAC (Version 2) protocol, each service provider[2] needs to be equipped with an authorization certificate, which usually needs to be renewed in regular time intervals either deploy an own eID-Server or use a corresponding eID-Service. While service providers usually need to apply for an authorization certificate at the German Federal Office of Administration ("Bundesverwaltungsamt", BVA) and pay a substantial service fee for the continuous renewal of the authorization certificate, there is an exception to this rule defined in § 21 (7) PAuswG, which states that public sector bodies in other MS are automatically entitled to access the identity information in the German eID by law. In this case the Federal Republic of Germany supplies the necessary certificates are provided in this case for free in addition to the 'German eIDAS-Middleware', which is available as Open Source. The user interaction either starts in the browser and invokes a separate eID-Client according to BSI TR-03124 on the corresponding platform. While on desktop operating systems the "eID-activation"[3] is realised via a localhost link, the analogous procedure on a mobile device uses "intents" to invoke mobile eID-Client such as the "AusweisApp2" and there is no need for a card terminal, if the mobile is equipped with NFC capabilities. In the mobile setting, the eID-functionality can be directly integrated into a "Service Provider App" in form of a library ("eID-Kernel"), which is available as Open Source[4]. Identification data between the service provider and the eID-Server or eID-Service is exchanged via SAML and there will be Open-Source libraries ("eID-Templates"), which make it easy to integrate the eID-functionality into popular Open Source web applications, such as Nextcloud, WordPress and TYPO3 for example.

3.5.1.7 Italian SPID and CIE

Italy has notified two eID schemes: Carta d'Identità Elettronica (CIE) is the public-sector issued national identity card and has been notified at LoA high. Sistema Pubblico di Identità Digitale (SPID) is a public-sector-initiated federation joined by numerous IdPs, many from the private sector, and has been notified at LoAs low, substantial, and high.

CIE is a contactless smartcard that, for user authentication, follows the European Citizen Card specification. It can be used with desktop computers equipped with a card reader and middleware integrating the card as a cryptographic token, but also using a mobile phone where an app "CieID" accesses CIE through NFC. Unique and persistent identifiers are based on the unique tax number. Integration of Italian public sector service providers is SAML-based, where an IdP service is operated by the Ministry of Interior. The CIE card can also be used to create advanced electronic signatures using a contact-less reader or an app and NFC.

[2] This is even true for device-internal EAC endpoints in high-end card terminals of "Kat-K" according to BSI TR-03119 for example.

[3] See https://www.openecard.org/en/ecard-api-framework/eid-activation/.

[4] See https://github.com/ecsec/open-ecard.

Draft

SPID is a federation of IdPs accredited by Agenzia per l'Italia Digitale (AGID), nine IdPs have been notified (see the table at the end of this section). The authentication means range from username and password (LoA low), username and password with SMS-OTP, mobile app-OTP, OTP-tokens, or call-back voice OTP (LoA substantial), or smartcards or HSMs that also are QSCDs for qualified electronic signatures (LoA high). The SPID identifiers are unique and persistent, but IdP-specific. As a user having several SPID eIDs, thus, has several identifiers, the SPID federation provides the tax number as optional attribute for identity matching in cross-border transactions. SPID can be used by public sector and by private sector relying parties and the integration is based on SAML.

3.5.1.8 Latvian eID karte and eParaksts

The Latvian eID started with the electronic identity card "eID karte", but soon has been complemented by eParaksts (Latvian for "electronic signature") which has been launched in 2018. eParaksts is public-sector operated by the Latvian State Radio and Television Centre LVRTC. It comes either as a smartcard or a mobile app-based solution "eParaksts+". These solutions have been notified at eIDAS LoA high. They support unique identification based on national registers and a qualified electronic signature. For the latter, the smartcards "eID karte" and "eParaksts karte" are the QSCD, for the mobile "eParaksts+ karte" the QSCD is a remote signature service, the user authorizes remote signature creation through the app.

Integration of the eID – both cards and the app – is using modules provided by LVRTC. Technically, integration is through REST APIs and OAuth 2.0. The system is browser-based both for identification and signature, browser plugins are provided for common browsers. Services are registered and provided an API access key, the scheme is open to public sector and private sector services.

3.5.1.9 Lithuanian eID card

Lithuania has notified its public-sector issued identity card Asmens Tapatybės Kortelė (ATK) at LoA high. ATK is a contact smartcard that is issued only to Lithuanian citizens and that is also a QSCD for qualified electronic signatures, a contactless interface is used for travel document functions.

Identification uses a unique and persistent national personal code. Client-side integration is through a middleware and browser plugins. The authentication process is through a component operated by the State Information Resources Interoperability Platform (SIRIP). The ATK scheme is currently restricted to public sector services.

3.5.1.10 Luxembourgian eID card

Luxembourg has notified its public-sector issued eID card at LoA high. It is issued just to Luxembourg nationals and is a contactless smartcard.

Unique identification is based on the citizen's national number, for cross-border transactions identifiers are derived relying-party-specific. The user's client needs a card middleware, the communication is based on the OASIS ChipGateway protocol. Luxembourgian public sector and private sector services can use the eID.

3.5.1.11 Netherlands eHerkenning and DigiD

The Netherlands notified two eID schemes: "DigiD" is an eID for natural persons at various LoAs, whereas LoA substantial and LoA high have been notified. "eHerkenning" is a federation of several IdPs to identify a business through representation by another person, it also supports LoA substantial and LoA high.

DigiD is a public sector issued scheme having different credentials ranging from username/ password and apps to smartcard systems. Both notified eIDs are app-based. At LoA substantial, the authentication process is carried out in the app and during enrolment NFC is used to bind the app to the driving licence or the ID card as physical documents. At LoA high, these two physical documents are used in the authentication process through NFC, the app can be seen as a contactless card reader and as implementing the connection protocols. The scheme is limited to public sector relying parties, no electronic-signature function is reported. SAML is recommended for integrating with

Draft

services, it is browser-based with the citizen either using the mobile phone's browser or a browser on a separate device. DigiD creates polymorphic pseudonymous identifiers per service. For eIDAS cross-border transactions, such a pseudonym is created per destination MS, uniqueness and persistence of the identifiers is guaranteed through the population register.

eHerkenning is a public-private partnership trust framework, which federates several accredited private sector IdPs. Notified authentication means at LoA substantial and LoA high are mainly apps or smartcards. Several of these authentication means are also QSCDs, for app solutions based on remote signing services. With supporting on-behalf authentication, mandate registers and authentication providers are linked through so-called recognition brokers. eHerkenning can be used by private-sector services, the eIDAS notification was however limited to public sector services. Integration for relying parties uses SAML. Unique identification is based on public registers, for natural persons using the same polymorphic pseudonyms as DigiD.

3.5.1.12 Portuguese CMD and CC

Portugal has notified two public-sector issued eID means, the citizen card "Cartão de Cidadão" and the mobile ID "Chave Móvel Digital", both at LoA high. A pre-notified attribute system "Sistema de Certificação de Atributos Profissionais" is pending legal clarification of its status in relation to eIDAS.

Both eID means are public sector driven and QSCDs supporting qualified electronic signatures, the mobile solutions using remote signing services. The mobile eID uses OTPs or the app for authentication at a central authentication server. The integration with public sector or private sector services is based on SAML. Persistent and unique identification is provided through the population register.

3.5.1.13 Slovak Citizen eCard

The Slovak Republic has notified its national ID card and residence permits at LoA high, thus a public sector issued eID means. It is a contact smartcard that also is certified as a QSCD for qualified electronic signatures. Usage is limited to public sector relying parties, integration is through SAML and a central authentication server. A persistent and unique identifier is provided by public registers.

3.5.1.14 Spanish DNIe

Spain has notified its public-sector issued electronic ID card "Documento Nacional de Identidad electrónico (DNIe)" at LoA high. DNIe is a dual-interface smartcard, it can be used as contact card and as contactless card, it also is certified as QSCD. Integration with public sector or private sector relying parties is through using the card's authentication certificate as a SSL/TLS client certificate, secure messaging with mutual authentication between the card and the service is supported. The Spanish eID supports persistent and unique identifiers based on the population register.

The following table gives an overview of the notified eIDs and links to its notification and documentation. The table summarizes information provided by the European Commission at the CEF DIGITAL eID user space.

Draft

Table 2: Overview of notified eID schemes

No	MS	eID scheme / eID means	LoA	OJEU	Further information
1	BE	Belgian eID Scheme FAS / eCards • Belgian Citizen eCard • Foreigner eCard	High	2018/C 464/08 (27.12.2018)	• Notification Form • Supporting Documentation • Opinion No. 7/2018
		FAS itsme • Belgian mobile ID	High	2019/C 425/06 (18.12.2019)	• Notification Form • Opinion No. 8/2019
2	HR	National Identification and Authentication System (NIAS) • Personal Identity Card (eOI)	High	2018/C 401/08 (07.11.2018)	• Notification From • Peer review Report • Pre-notification supporting documents • Opinion No. 4/2018
3	CZ	National identification scheme of the Czech Republic CZ eID card	High	2019/C 309/09 (13.09.2019)	• Notification Form • Opinion No. 2/2019
4	DK	NemID • Key card (OTP) • Mobile app • Key token (OTP) • NemID hardware • Interactive Voice/Response (OTP) Magna key card (OTP)	Substantial	2020/C 116/05 (08.04.2020)	• Pre-notification Form • Opinion No. 1/2020
5	EE	Republic of Estonia • ID card • RP card • Digi-ID • e-Residency Digi-ID • Mobiil-ID Diplomatic identity card	High	2018/C 401/08 (07.11.2018)	• Notification From • Pre-notification supporting documents • Opinion No. 5/2018

Draft

No	MS	eID scheme / eID means	LoA	OJEU	Further information
6	DE	German eID based on Extended Access Control • National Identity Card • Electronic Residence Permit eID Card for Union Citizens and EEA Nationals	High	2017/C 319/03 (26.09.2017) 2020/C 432/07 (14.12.2020)	• Documentation about German eID notification • Opinion No. 1/2017
7	IT	SPID – Public System of Digital Identity • Aruba PEC SpA • Namirial SpA • InfoCert SpA • In.Te.S.A. SpA • Poste Italiane SpA • Register.it SpA • Sielte SpA • Telecom Italia Trust T. S.r.l. • Lepida SpA	Low, Substantial, High	2018/C 318/02 (10.09.2018) amended by 2018/C 344/09 (26.09.2018) 2019/C 309/09 (13.09.2019)	• Notification Form • Supporting Documentation • Opinion No. 1/2018 • Opinion No. 4/2010 (amendment)
		CIE - National ID card	High	2019/C 309/09 (13.09.2019)	• Notification Form • Opinion No. 4/2019
8	LV	Latvian eID scheme (eID) • eID karte • eParaksts karte • eParaksts karte+ eParaksts	Substantial, High	2019/C 425/06 (18.12.2019)	• Documentation about the LV eID scheme • Opinion No. 7/2019
9	LT	Lithuanian National Identity card (eID / ATK) Lithuanian National Identity card (eID / ATK)	High	2020/C 276/02 (21.08.2020)	• Opinion No. 3/2020

Draft

No	MS	eID scheme / eID means	LoA	OJEU	Further information
10	LU	Luxembourg national identity card (eID card) Luxembourg eID card	High	2018/C 401/08 (07.11.2018)	• Peer Review Report • Opinion No. 3/2018
11	NL	Trust Framework for Electronic Identification (Afsprakenstelsel Elektronische Toegangsdiensten) Means issued under eHerkenning (for businesses)	Substantial, High	2019/C 309/09 (13.09.2019)	• Pre-notification Form • Peer review report • Supporting Documentation • Opinion No. 3/2019
		DigiD	Substantial, High	2020/C 276/02 (21.08.2020)	• Notification Form • Opinion No. 4/2020
12	PT	Cartão de Cidadão Portuguese national identity card (eID card)	High	2019/C 75/04 (28.02.2019)	• Documentation about Portuguese eID • Supporting Documentation • Opinion No. 6/2018
		Chave Móvel Digital Portuguese mobile ID	High	2020/C 116/05 (08.04.2020)	• Notification Form • Opinion No. 2/2020
13	SK	National identity scheme of the Slovak Republic • Slovak Citizen eCard Foreigner eCard	High	2019/C 425/06 (18.12.2019)	• Documentation about the SK eID scheme • Opinion No. 06/2019
14	ES	Documento Nacional de Identidad electrónico (DNIe) • Spanish ID card (DNIe)	High	2018/C 401/08 (07.11.2018)	• Notification From • Opinion No. 2/2018

Draft

3.5.2 Non-notified European eID

This section discusses European eID solutions beyond the formally notified ones. We concentrate on national solutions, but particularly also on interesting mobile solutions from the private sector that do not have a link to national programmes. We start with two national eIDs, one in the pre-notification process and thus expected to soon move to notified eIDs, and one that actual has been notified but due to Brexit no longer falls under the eIDAS regime. We then continue with national initiatives where notification has been announced. This gets complemented by private mobile eID services that have been either identified by the mGov4EU consortium as interesting show cases or have been brought to us through a survey.

The description addresses the same questions as for the notified schemes above, although slightly modified, as an eIDAS LoA only exists once an eID scheme is formally notified. Also, the notion of a persistent identifier and identity matching may be less relevant in some schemes not having the long-term and cross-sectoral relationships that government services have with citizens. The slightly modified questions to be answered per eID scheme are:

- What basic technology is used by the eID scheme (card, mobile, or others)?
- What is a comparable eIDAS Level of Assurance, if applicable?
- Are electronic signatures supported by the credential?
- Is it a public-sector or private-sector driven scheme?
- How is integration with relying parties done?
- Is the eID scheme limited to relying parties from the public sector, or is it open to the private sector as well?
- How can identity matching be done, if applicable and if identifiers are not persistent or unambiguously unique?

3.5.2.1 Swedish Bank ID and Freija

When drafting the present contribution, Sweden has already pre-notified two eID means of its eID scheme “Svensk e-legitimation”[5]. Svensk e-legitimation is a trust framework that governs requirements that IdPs need to fulfil and are audited and supervised against. The trust framework defines four assurance levels based on an impact and risk rating in six categories. The Swedish assurance levels 2, 3, and 4 can be argued to map to eIDAS LoA low, substantial, and high.

Audited IdPs that meet the requirements of the trust framework can join the national federation “Sweden Connect”. Public sector and private sector relying parties can be integrated using SAML. Unique and persistent identification is assured through public registers, but with residents and non-residents being assigned different identifiers, which can require reconciliation, if the latter become residents.

The pre-notification covers two IdPs: BankID[6] and Freja[7], both private sector solutions. BankID can be a smartcard, a smartphone app, or a middleware application on the desktop. Freja is based on a smartphone app. No QSCD certification of these solutions is known. As the eIDAS peer-review process of these solutions is ongoing, the final notification results including the confirmed LoA statement of these solutions by Sweden needs to be awaited.

3.5.2.2 GOV.UK Verify

The UK had notified the eID framework GOV.UK Verify[8] at LoA low and LoA substantial under eIDAS. With Brexit, however, the mutual recognition obligations of eIDAS no longer apply. The eID means are therefore described in this section on non-notified eIDs.

[5] See https://www.e-legitimation.se/en

[6] See https://www.bankid.com/

[7] See https://frejaeid.com/en/home/

[8] See https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

Draft

GOV.UK Verify is a trust framework governed by the public sector, with different private sector IdPs. The technical architecture consists of an Identity Assurance Hub operated by the public sector that IdPs and public sector relying parties can interface with using SAML. Until March 2021, five IdPs existed, in March 2021 this has been reduced to two: Digidentity and Post Office, both providing a smartphone app. No QSCD certifications are known. Unique identification is ensured on a per IdP basis, national services for identity matching exist.

3.5.2.3 ID Austria

The Austrian eID[9] has been introduced as a technology-neutral concept, supporting smartcard-based and mobile eID from its beginning. As the Austrian eID undergoes a major revision which will replace the current scheme in the course of 2021 and which due to low take-up of smartcards eID will solely be a mobile solution, we limit this overview to this new "ID Austria".

ID Austria is a mobile eID which is governed by the public-sector with a private-sector trust service provider for qualified electronic signature services. The system is open to public-sector and private-sector relying parties. Integration for browser-based services is done via SAML or OpenID Connect, for mobile services also through app-app communication. Unique and persistent sector-specific or private-organisation-specific identifiers are provided through public registers. eIDAS pre-notification is planned at LoA high in 2021.

3.5.2.4 nextAuth

NextAuth is a private initiative providing mobile authentication and mobile advanced signature services. Authentication is based on a specific cryptographic key exchange protocol (Krawczyk, 2003), mutual authentication of the user's app and the relying is provided. Integration with relying parties is through a nextAuth server component. NextAuth targets organisations that need authentication solutions for their staff or clients, but also identity-as-a-service providers. It thus less markets to end users, a LoA mapping that does not just assess the technical security of the app but also identification strength during enrolment of users will thus depends on how these nextAuth clients integrate the system.

3.5.2.5 Norwegian ID-porten

Norway has introduced ID-porten as a login portal to public services. Relying parties integrate with ID-porten using SAML or OpenID Connect. The portal federates several public-sector or private-sector IdPs. Most IdPs besides the public ID-porten also provide authentication services for private-sector relying parties. For the public-sector governed scheme, unique and persistent identification is supported through registers.

The currently connected IdPs are MinID, BankID, Buypass ID and Commfides. MiniID is issued by the public-sector and relies on a username-password scheme with SMS-OTP or PIN-lists. BankID comes either with an OTP-generator or as a smartphone app. Buypass ID either uses smartcards or a smartphone app. Commfides delivers a USB stick accessed through a browser plugin. The federation has four Levels of assurance. MinID operates at assurance level 3, BankID, Buypass ID and Commfides support the highest assurance level 4. A mapping of these levels to eIDAS LoA is pending Norway's pre-notification under eIDAS. Some of the solutions support advanced electronic signatures, which under Norwegian legislation are equivalent to handwritten signatures.

3.5.2.6 OPTIMOS 2.0 - German Mobile eID

OPTIMOS 2.0[10] is a German mobile eID project by public and private partners which, was initially funded by the German Ministry of Economics and Energy (BMWi) and which now is in the process of being integrated into the existing German eID infrastructure and aims at satisfying the criteria of eIDAS LoA substantial or high, if possible. Its goal is to abstract from vendor specific smartphone

[9] See https://www.oesterreich.gv.at/id-austria.html

[10] See https://www.bundesdruckerei.de/en/innovations/optimos

Draft

features and in the long term support all mobile devices with secure elements (eSE or eUICC). A user, who wants to register for the Mobile ID, has to be identified and authenticated via its regular German eID. The user's attributes are used to generate a derived identity, which is deployed into the secure element of the user's mobile device using a Trusted Service Management System (TSMS). Once stored, the derived identity can be used to authenticate to public-sector or private-sector SPs who integrate with the German eID scheme. The project conceptually allows for applets beyond eID functions and hence electronic signatures could be supported but are currently not in the scope of the project.

For the integration of the Mobile-ID, SPs must perform two steps. First, they have to supply service-specific Applets to the Service-Provider-TSMS. These Applets – personalized with the user's identity information before deployment - are stored one the secure elements via TSMS. Second, they have to integrate the TSMS into their application. Therefore, a TSM-SDK is provided. Due to the use of the existing German eID infrastructure, the integration process for online authentication is the same as described for the German eID scheme in the previous section on notified eIDs, so are identifiers and identity matching aspects.

3.5.2.7 Student eCard / StudIES+

The Student eCard in the StudIES+ project[11] is an example of a sectorial mobile identity initiative. Being a project and thus not yet a full production system, the project ambition nicely shows what mobile services could provide.

The project aims at facilitating student mobility like in the Erasmus+ programme by deriving identity from eIDAS eIDs to be used on the smartphone and to integrate these together with electronic signatures in workflows of higher education institutions. The derived identity on the smartphone can then be used in online services like campus online services, or as visual identity like in a library. The project also supports signature functions. Being a project and no production service no statement on its LoA can be made.

3.5.2.8 SkIDentity

SkIDentity provides "Mobile eID as a Service" by allowing to derive so called "Cloud Identities"[12] from a variety of card-based European eID means and other authentication services. Unlike the name may suggest, a "Cloud Identity" is stored and cryptographically anchored with best-effort to the device of the user. The user-centric credential may additionally be bound to FIDO U2F tokens to provide an additional level of security. The initial system was created with support from the German Ministry of Economics and Energy within the "Trusted Cloud" Programme and was certified by the Federal Office for Information Security according to ISO 27001 based on IT-Baseline protection as well as by TÜV Informationstechnik GmbH (TÜViT) according to the Trusted Cloud Data Protection Profile (TCDP). SkIDentity is tightly integrated with the Open eCard client technology and provides the basis for innovative eID-based mobility services in the FiftyFifty Taxi system[13].

3.5.2.9 Verimi

Verimi[14] is an example of a commercial app-based ID and signature solution. The Verimi provider operates an authentication service. Relying parties integrate the eID using OpenID Connect and OAuth 2.0. Qualified electronic signatures are supported by authorising a signature using the Verimi eID. The solution addresses the German market, services where it can be used are mainly private-sector services related to online-banking or telecom operators, but also a few regional public services. As not being notified, no statement on eIDAS LoA can be made.

[11] See https://studies-plus.eu/

[12] See https://www.skidentity.de/en/help/faq1#faq2.

[13] See https://ec.europa.eu/futurium/en/blog/eidas-action-case-fiftyfifty-taxi-app.

[14] See https://verimi.de/en/

Draft

3.5.3 Beyond Europe

In this section, we complement the survey of European eID solutions by looking abroad. We focus on mobile solutions and selected approaches that in some aspects differ or complement what has been discussed for European eIDs. Compiling a comprehensive survey of worldwide mobile eID is almost impossible and has little merit if it repeats aspects also given with solutions already described. We therefore searched for approaches that have an interesting aspect not seen in those described so far.

For each solution we aim at answering the same questions as we did for the non-notified European eIDs, except for the question on identity matching or relying party integration. This as these questions relate to actual integration in eIDAS or an mGov4EU pilot, which is not in scope.

- What basic technology is used by the eID scheme (card, mobile, or others)?
- What is a comparable eIDAS Level of Assurance, if applicable?
- Are electronic signatures supported by the credential?
- Is it a public-sector or private-sector driven scheme?
- Is the eID scheme limited to relying parties from the public sector, or is it open to the private sector as well?

Given that technical documentation was not available for all the solutions that are described, not all questions could be answered for each. This, however, is not seen limiting to mGov4EU, as the purpose was not elaboration on these non-European solutions influencing our architecture, but to search for interesting aspects that might go beyond what we have as comfort zone of notified eIDAS eIDs.

3.5.3.1 Arizona

The Arizona Department of Transportation launched an app in 2020 that allows access to vehicle or driver licence information, or to start services like licence renewal. This limited scope of one department issuing an app-based means to access its own services is not seen as a general-purpose eID. Some other services like voter registration are, however, supported by the platform and federated authentication to other eGovernment services is planned.

An interesting development why the solution has been included here is the plan to enhance the functions by a mobile driver licence in 2021. This is following the ISO/IEC 18013-5 standard (cf. section 3.4.2.5.1) and shall support both online authentication at eGovernment portals and physical identification.

3.5.3.2 Azerbaijan Asan Imza

Azerbaijan has a smartcard-based eID (e-IMZA)[15] that also supports electronic signatures. A mobile eID and electronic signature solution Asan Imza has been introduced through a public-private partnership. The solution is based on a specific SIM card with crypto functionality, the solution claims compliance with eIDAS qualified signature requirements (for formal eIDAS equivalence, a third country agreement with the EU would be needed). Technically, Asam Imza can be compared with the Estonian Mobiil-ID (cf. section 3.5.1.6). Unique identification is provided through public registers.

Asan Imza can be used in eGovernment services, but also in private-sector services, like being supported by major banks. An interesting aspect is mResidency, as enrolment to this mobile solution can be carried out at diplomatic representations or consulates by non-residents and foreigners. This would, e.g., allow to open a business in Azerbaijan remotely.

[15] See http://e-imza.az/en/about

Draft

3.5.3.3 Canada

Canada introduced the Pan-Canadian Trust Framework[16] first for public-sector services and later for private-sector relying parties. It is a federation of identity providers that includes various credentials, several being app-based. An interesting approach is verified.me which operates a network of solution providers and which is based on blockchain. The solution provides end-to-end encrypted credentials, i.e., no actor in the ecosystem can get a complete overview of the transactions.

3.5.3.4 Mobile Connect

Not attributed to a specific country, GSMA's Mobile Connect (cf. section 3.4.2.3.3) is an ecosystem that is supported by more than 70 mobile network operators, thus private-sector driven. When completing this deliverable, the Mobile Connect developer portal reports for status "Live, open for 3rd party use" and service level "Authenticate Plus" providers in Argentina, Chile, Colombia, Ecuador, Finland, France, Germany, Netherlands, Peru, Poland, Spain, and Sri Lanka. The service level "Authenticate" just confirms that a user is in possession of a mobile. More interesting as a mobile eID is "Authenticate Plus", as it is a two-factor authentication prompting the user for a PIN, thus a wilful act by the user to authenticate. The integration with relying parties is through OpenID Connect.

3.5.3.5 Nigerian NIN

The Nigerian ID programme is governed by the Nigerian Identity Management Commission, thus public-sector driven. Identity management is based on a unique national identity number (NIN), credentials range from a paper NIN-slip (sort of a photo ID with the NIN printed on it), an enhanced machine-readable NIN-slip with a QR code, and in its eID-version a smart-card eID and a mobile ID app.

Interesting aspects are that the smartcard eID was charged to the citizen, whereas the mobile ID is provided free of charge. Aside online authentication, the eID card can be used for payments or cash withdrawal at ATMs (no information was available whether this is also planned for mobile ID). A further interesting aspect is that the mobile ID can also be used in conventional physical presence processes, as the NIN and QR-code can be shown like with the enhanced paper NIN-slip.

A further interesting aspect is that Nigeria plans to apply the OSIA Initiative principles and specifications (see section 3.4.1.6).

3.5.3.6 Oman TAM

The Sultanate of Oman introduced a smart card based eID, it is based on a national PKI providing authentication and signature certificates. Oman, however, also was among the first Middle East countries to complement the smartcard by a mobile ID. It is a public-sector driven mobile ID that is provided by licensed and accredited mobile network operators. The solution requires specific SIM cards. Both the eID card and the mobile ID provide electronic signatures comparable to qualified electronic signatures under eIDAS. An interesting aspect is that it is a government funded system that is free of charge for citizens, as well as for the public-sector relying parties.

3.5.3.7 Singapore SingPass

SingPass[17] is a public-sector national identity system. Originally launched 2003 as a username password authentication system it evolved to a multi-factor authentication service (using OTPs) and now also a mobile ID app. It can be used in public-sector and private-sector online applications. Integration is using OpenID Connect. Electronic signature functions are supported. Remarkable is that the app can also be used as a physical identification document. It is a government funded model free of charge both for citizens and for relying parties.

[16] See https://diacc.ca/

[17] See https://www.singpass.gov.sg/main

Draft

3.6 Findings of the eID survey

The conducted survey has approached the topic electronic identification (eID) from different perspectives. First, relevant literature has been reviewed, whereas focus has been put on scientific contributions. Then, an overview of relevant eID frameworks has been provided. In this context, both policy and technical frameworks have been considered. Finally, existing eID solutions in Europe and beyond have been surveyed to complement the picture of the current state of the art.

From the conducted survey and the obtained comprehensive overview, several findings can be derived that are directly relevant for upcoming activities in mGov4EU. Relevant findings are summarized below.

eID as global phenomenon. From the conducted survey it becomes apparent that eID is a topic of interest all over the world. Although the survey has focused by intention on Europe and the EU, selected solutions and frameworks beyond this scope have been considered as well. This has revealed that the need for secure and reliable eID solutions exists on all continents and in most countries. This applies especially to Europe and the EU, where the eIDAS Regulation provides a strong policy framework for a variety of technical eID solutions and their interoperability. The global relevance of eID becomes also apparent from the conducted review of related literature. This review shows that the scientific interest on eID concepts and solutions is not restricted to a certain area or region but applies globally.

Strong policy and technical frameworks. In general, the EU and its Member States benefit from a strong policy framework with regard to eID. The key framework in the EU is the eIDAS Regulation, which ensures interoperability between the eID solutions of different EU Member States and hence enables authenticated cross-border access to services. Relevant legal and policy frameworks are supported by various technical frameworks (standards, norms, technical protocols, etc.), which provide a solid technical basis for the development and operation of eID systems. Concerning technical frameworks, it can be observed that existing frameworks are less complete and mature when it comes to mobile use cases. This especially applies to so far only rarely applied use cases, e.g., eID solutions supporting direct interactions between multiple mobile apps on a mobile device or solutions incorporating cutting-edge concepts like self-sovereign identities. The conducted survey has shown that mGov4EU can break new ground here.

Shift towards mobile eID solutions. Although mGov4EU has a clear focus on mobile solutions, the survey on eID has intentionally chosen a broader scope and considered eID solutions in general – irrespective of their underlying technical concept and realization. This way, it became apparent that classical technologies such as smartcards still play an important role in several public sector driven eID solutions. However, it can also be observed that mobile eID solutions incorporating a mobile device during user authentication or even being fully tailored to mobile-only use cases experience a growing popularity. To date, both classical and mobile eID solution exist next to each other. However, it can be observed that the majority of newly introduced eID solutions are already based on mobile technologies and/or support mobile use cases. Hence, mGov4EU, which has its focus on mobile solutions, can contribute to an ongoing trend.

Heterogeneous landscape regarding the technical realization of mobile eID solutions. While classical smartcard based eID solutions resemble each other to a certain extent (at least concerning the use of the smartcard), the conducted survey has revealed considerable heterogeneity regarding the concrete technical implementation of mobile eID solutions. This seems comprehensible, as modern mobile devices provide much more different features and capabilities compared to, e.g., a smartcard. Surveyed mobile eID solutions make use of integrated secure elements, employ SIM cards, or rely on remote hardware security modules. This heterogeneity needs to be considered when achieving interoperability between such – potentially different – technical solutions.

SAML 2.0 and OIDC as de-facto standards. The compiled overview of currently available eID solutions has revealed that the protocols SAML 2.0 and OpenID Connect (OIDC) have evolved to de-facto standards that are used by nearly all surveyed schemes to connect identity providers (of eID systems) with service providers. The above-mentioned shift towards mobile solutions will

Draft

potentially raise interesting challenges in future in this regard. While SAML (and later SAML 2.0) has been the predominating protocol used in classical browser-based usage scenarios, this protocol is less frequently supported in mobile scenarios. There, OIDC is the usual choice. This might, for instance, become a challenge once mobile-only usage scenarios will be realized in a cross-border context, using the existing eIDAS interoperability framework that is currently based on SAML 2.0. mGov4EU can contribute to this issue by investigating and testing different approaches to achieve OIDC-based mobile-only solutions in a cross-border context relying on a framework that supports SAML 2.0 only.

App2App and SSI solutions still underdeveloped. App2App scenarios, i.e., scenarios in which an app on a mobile device calls another mobile app on the same device, have turned out to be hardly supported by current mobile eID solutions. This is not surprising, as mobile platforms such as Android and iOS do not heavily promote this kind of App2App interaction. Also, technical capabilities to implement App2App communication on mobile platforms exist but are limited. Still, in the context of eID systems, App2App scenarios can be useful for several use cases, e.g., when a service-provider app wants to request eID attributes from an eID app on the same device in an offline scenario. For such offline scenarios, also SSI-based approaches can be useful to enable a secure storage and provisioning of eID attributes. However, the conducted survey has shown that SSI and related concepts have not yet made their way into productive eID solutions. So far, these concepts are rather tested and piloted in research projects and discussed in scientific publications only. mGov4EU can contribute to this regard and pave the way for the integration of App2App approaches and SSI concepts into real-world eID solutions.

Need to distinguish between the public and the private sector. The conducted survey has shown that current eID solutions are driven by both the public and the private sector. In this regard, the situation heavily depends on the respective country and its national eID strategy. One also needs to distinguish whether available eID solutions are open to all service providers or restricted to a certain class of relying parties. Here, the conducted survey shows that several national (i.e., public sector driven) eID systems can be used by public-sector service providers only. Again, this heavily depends on the respective country and its eID strategy.

Majority of notified eID schemes support LoA high. Several EU Member States have already notified one or more eID scheme(s) following the eIDAS notification process. Having a more detailed look at these notified schemes reveals that most of them support LoA high. Only a few schemes have been notified with a lower LoA (i.e., Substantial or Low). However, at least in some cases it can be observed that the lower LoAs are assigned to mobile eID solutions. mGov4EU can tackle this issue and, e.g., by advancing mobile cutting-edge technologies and making them ready for use in productive eID solutions, ensure that mobile eID solutions remain compliant with requirements associated with LoA high.

Only partial support for qualified electronic signatures. In general, eID and electronic signatures represent two distinct concepts that do not necessarily need to have strong interdependencies. Still, several eID schemes do not only enable end users to securely authenticate at service providers but also enable them to create qualified electronic signatures (QES). The combination of eID and QES is still common for several smartcard-based solutions, as appropriately certified smartcards can act as qualified signature creation devices (QSCD) as defined by the eIDAS regulation. For mobile eID schemes, the situation is more complex, as there are various technical alternatives (remote HSM, SIM, etc.) to realize the required QSCD. Overall, the conducted survey has shown that QES support is available in several eID schemes (mobile schemes and classic schemes). However, it must not be expected that QES support is universally available and supported by all schemes. Also, it is important to note that the eIDAS protocol does not support the request of a QES in cross-border scenarios. Through its mobile signature pilot, mGov4EU can investigate possibilities to include QES in mobile use cases.

Challenges regarding identity matching. When it comes to interoperability of eID schemes and systems, the unambiguous identification of end users is a crucial requirement. Unique and persistent user identifiers are a reliable means to achieve this. However, the conducted survey of notified eID schemes in EU Member States has shown that at least some of these schemes do not provide

Draft

persistent identifiers. For instance, there are schemes that supply one and the same person with multiple (unique) identifiers at the same time (e.g., when multiple identity providers are involved). In other schemes, a person has only one identifier at a time, but this identifier is replaced in regular intervals (e.g., when the person receives a new credential). Non-persistent identifiers make it difficult to determine whether the person participating in the current session equals the person from a previous session. In the worst case, one and the same person is assigned with multiple eIDs. This problem is potentially aggravated in mobile scenarios that require the offline provision of eID attributes. If such scenarios require for security reasons the use of derived identifiers, successful matching of identities might become even more challenging. By investigating the use of SSI and related concepts, mGov4EU can identify further challenges concerning identity matching in mobile use cases, come up with solutions to these challenges, and hence improve identity matching in a cross-border context in general.

Overall, the conducted survey on electronic identification (eID) has yielded a solid overview of the current state of the art. By having a more detailed look at scientific literature, policy and technical frameworks, and eID schemes in Europe and beyond, several interesting and useful findings could be derived. These findings point to directions, where mGov4EU can advance the current state of the art, and where major challenges are to be expected.

Draft

Chapter 4 Cross-border data exchange

4.1 Introduction and methodology

The Digital Single Market is an initiative in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence (European Commission, 2015). The Digital Single Market was already part of the strategy of the European Commission 2014 - 2019 and the work is continued as part of the EC priorities for 2019 - 2024. One of these priorities is to make Europe fit for the digital age and one of the pillars of the Digital Single Market strategy is to create a better access for consumers and businesses to digital goods and services across Europe. eGovernment as corner stone of the activities in digital Europe can provide a wide variety of benefits including more efficiency and savings for governments and businesses, increased transparency, and greater participation of citizens, e.g. in political life and cross border services. The mGov4EU project follows a citizen-centric approach to provide a bridge between eIDAS and the Single Digital Gateway (SDG) in order to enable Mobile Cross-Border Government Services for Europe.

The methodology is based on preliminary literature analysis of the cross-border data exchange systems. Besides that, to ensure the interoperability with other digital public services, the European Interoperability Framework (EIF) and its layers are used as a basis for the structure of this chapter (Figure 3). The structure of the analysis was based on the interoperability layers presented in the EIF. Furthermore, the approach for the related integrated public services will be explained.

4.2 Policy layer of interoperability

This section presents the policy initiatives and legislation's background addressing the interoperability policy and cross-border data exchange on the EU level. Since interoperability is a necessary condition for reliable and trustworthy cross-border access to procedures and cross-border data exchange, this section is inspired by the interoperability model of the European Interoperability Framework; more specifically, it includes interoperability governance and integrated public service governance.

Draft

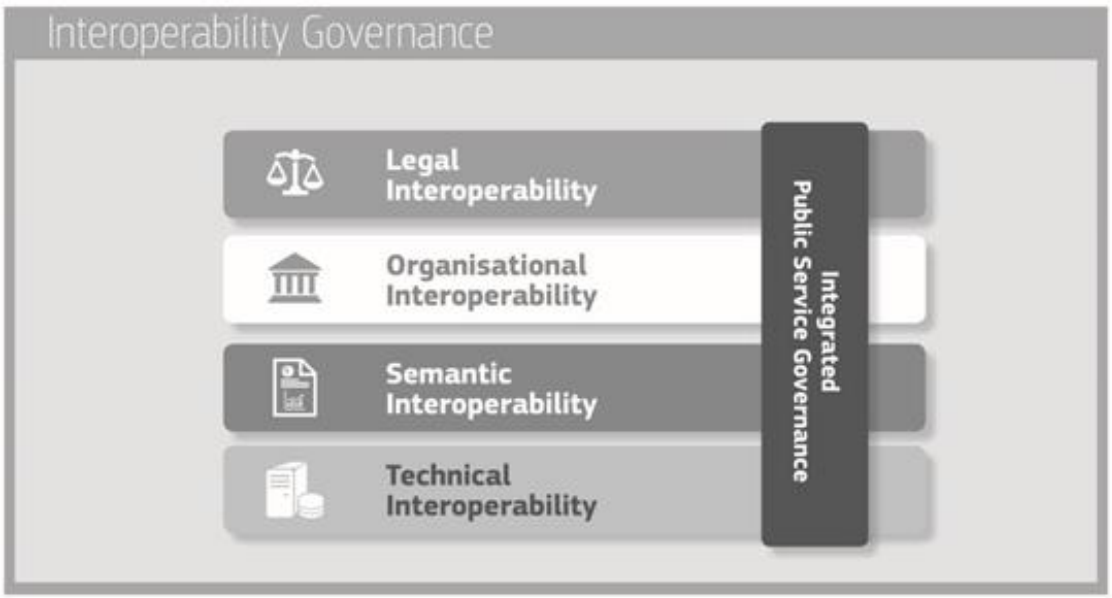

Figure 3: Interoperability model (European Commission, 2017)

4.2.1 Interoperability governance – policy layer

As defined in the EIF, interoperability governances, among other things, all decisions on interoperability, policies and institutional agreements that enable interoperability at the national and EU level (European Commission, 2017). This subsection describes the policies and initiatives of the EU level in ensuring the digital transformation within the EU.

One of the main priorities at the EU level, inter alia, is to achieve the Digital Single Market which will enable citizens and business to access and exercise online activities across EU. The European Commission adopted the Digital Single Market Strategy communication to harmonise the initiatives and incentivise the development of digital transformation. A Digital Single Market can be understood as one ecosystem in which the citizens and business can assess the online services under fair competition conditions and personal data protection, irrespective of their nationality or place of residence (European Commission, 2015). One of the barriers that are hindering the development of the Digital Single Market is the lack of open and interoperable systems and services and the lack of common data portability infrastructures, as addressed in the Digital Market Strategy. To overcome these barriers, one of the suggested solutions in this strategy was that the needs of business and citizens in the cross-border setting could be best addressed by building online services on the existing building blocks of the Connecting Europe Facility programme, with further integrating the existing platforms, portals, networks and systems into one Single Digital Gateway (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, 2018).

The EU has adopted the eGovernment Action plan 2016 – 2020 to set up conditions and define actions to achieve the Digital Single Market's strategic objectives, such as modernising public administrations, achieving cross-border interoperability and enabling easy interactions with the citizens (European Commission, 2016). The eGovernment action plan's main aim is to enable citizens and business to fully benefit from the digital public service that should be available across the EU for all EU citizens. One of the leading suggestions and actions to achieve the objectives was that the public administrations should make relevant digital public services for cross-border users and prevent further fragmentation in the digital environment (European Commission, 2016).

The latest policy initiative by the EU is the Digital Europe Programme for 2021 - 2026, which aims to reinforce the impact of the Digital Single Market's policy achievements. The Digital Europe Programme's primary objectives are to create investment opportunities within the EU, national, regional and local level in the critical technological industries (Digital Europe Programme, 2020). This investment programme is the key programme to achieve seamless cross-border public services in the EU in the next following years. To achieve this objective, the draft orientations draft work programme for 2021-2022 suggested, among other things, enabling citizens-centric digital public services. Three key priority actions are agreed on to achieve the objective of citizen-centric digital public service. First is the creation of the Digital transformation platform, second the rollout of the once-only principle (OOP), and third the implementation of the interoperability incubator. Within these priority actions, the European Commission will deploy and support the full integration of the CEF Telecom building blocks, ISA^2 actions and the European Data portal into one ecosystem Digital Transformation Portal, which will provide the basis especially for the implementation of the OOP in the cross-border settings under the Single Digital Gateway.

Furthermore, EC will continue supporting the further implementation of the once-only infrastructure and technical systems at the regional and local level under the Single Digital Gateway. Finally, an interoperability incubator will enable innovation in the digital government services by supporting the innovative technologies and enable pilot programmes for the new interoperable public services. (Digital Europe Programme, 2020). Proposed actions in the Digital Europe programme will further enable interoperability among the public administrations at all administration levels and achieve seamless cross-border digital public services.

Next to the initiatives/policies mentioned above by the European Commission, an important document for the development of the digital public services in the EU is the ministerial document,

Draft

the Tallinn Declaration on eGovernment, adopted in 2017. Having in mind that the eGovernment Action plan is extensive but that there is a need for more collaboration in the EU, ministers of the EU MS agreed on the shared vision and actions to enable and provide borderless and interoperable digital public services to all citizens and business (European Commission, 2017). Among the common principles for digital public services, Tallin Declaration also addressed specific actions that the MS will work on to achieve the objectives. In particular, they agreed to collaborate to implement the OOP for the key public services and also to adhere to EIF for the cross-border digital public services to achieve the principle of interoperability by default.

Recognising the importance of the united support and political commitment towards the digital transformation of the public services and the importance of the goals addressed in the Tallinn Declaration, ministers of the MS agreed to continue and further support the development of the digital public services ecosystem in the EU. The Berlin Declaration has been adopted with the objective to achieve value-based digital transformation by supporting and strengthening digital participation and inclusion in the EU (European Commission, 2020). They agreed that they would continue to coordinate cross-border interoperability and also strengthen the EIF. In particular, one of the priorities is to strengthen Europe's digital sovereignty and interoperability. To achieve this priority, MS will collaborate to reduce the administrative burden on European citizens and businesses and promote the cross-border implementation of the OOP by supporting interoperability by design policies and solutions. Furthermore, the Berlin Declaration confirms the value and importance of the mgov4EU project by acknowledging that most citizens use mobile devices. The signatories agreed to include, next to the electronic government, the mobile government's concept when developing interoperable digital public services. Proper electronic government concepts and solutions will provide a sound basis for mobile government as a next step towards a digital society.

4.2.2 Integrated public services governance at the EU level

This subsection describes the policies and initiatives that ensure “integration, seamless execution, re-use of services and data, and development of new services and building blocks” (European Commission, 2017, p. 22). EU digital public services are achieved by many interconnections and collaboration of multiple organisations to provide digital public services, which requires coordination and governance on the EU level. Thus, in the cross-border data exchange, the EU policies and initiatives that enable the coordination and governance of the EU, digital public services will be described.

Next to the policies and resolutions mentioned above in the field of the eGovernment and interoperability, European Union has also addressed the governance of the interoperable European Public Services by creating the main funding programmes for interoperability "Interoperability solutions for public administrations, businesses and citizens – ISA^2" and the "Connecting Europe Facility – CEF".

These programmes aim to facilitate and enable the cross-border digital public services between the public administrations at the cross-border, national, regional and local level (Wimmer et al., 2018). The ISA^2 programme was adopted in 2015, and it was running from 2016 until 2020, intending to support the development of cross-border digital interoperable solutions for public administration. ISA^2 is developing interoperable solutions under 54 actions that are addressing the Legal, Organisational, Semantic and Technical interoperability and these solutions are being available open-source and free to use. Furthermore, it is found that in the absence of ISA^2, the overall objectives for cross-border interoperable public services would not be achieved by only national or subnational interventions. Consequently, the coordination and development of the interoperability solutions and services by ISA^2 is significant in achieving cross-border interoperability within public administrations in the EU. Finally, it has been shown that ISA^2 has contributed to improving the cross-border interoperability in the EU, by raising awareness on the topic of interoperability and by facilitating the exchanges between MS (Iacob et al., 2019).

Similarly, the CEF is a funding programme that supports the development of the infrastructure and technical solutions for digital public services, facilitating cross-border interactions between public administrations, citizens and businesses (CEF Digital). CEF supports cross-border interactions by

Draft

deploying key building blocks Digital Service Infrastructures (DSIs) to create an interoperable European digital ecosystem for public administrations (CEF Digital). The value of these building blocks is the reusability and the variety of its use as it can also be integrated into other IT projects and combined with each other (CEF Digital). Building blocks that CEF has been developed, inter alia, are eID, eSignature, eInvoicing, eDelivery, Automated Translation, EBSI, the OOP.

Alongside the EC funding programmes, EC has addressed the interoperability of public services in the EU level by adopting the revised European Interoperability Framework in 2017. The EIF provides guidance and recommendations to public administrations on developing and achieving interoperable digital public services. The EIF is a good basis to "ensure interoperability and common approaches to data infrastructures at EU and in the MS" (Wimmer et al., 2020) (European Commission, 2019). In the EIF, interoperability is defined as "the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems." (European Commission, 2017). The purpose of the EIF is to inspire public administrations to develop and deliver interoperable digital public services to other public administrations, business and citizens; to provide guidance to public administrations on how to design their own national interoperability framework; and lastly but not least, to contribute to the establishment of the Digital Single Market by creating and supporting cross-border interoperable European public services. Three main elements of the EIF, are the core interoperability principles, interoperability layers (Legal, Organisational, Semantic and Technical) and integrated public services model. One of the recommendations, inter alia, within the EIF is addressing the functioning of the Digital Single Market and the data exchange systems, in which is recommended that the designers of public services should address the data portability infrastructures in order to avoid lock-in and to support the free movement of data. As previously mentioned, the structure of this chapter is inspired by the EIF interoperability model in order to present the state of the art of the cross-border data exchange systems in the EU while having in mind the principle of interoperability-by-design.

At the moment of writing, the EC is conducting the final evaluation of the ISA^2 programme and EIF, with the impact assessment of the future interoperability strategy for the EU. The results of this project will serve as the reference point for the updated European Interoperability Framework.

4.3 Legal interoperability

Following the overarching political initiatives in the field of eGovernment and also the funding programmes and frameworks in the field of interoperability, in this part, the main focus will be on the legal interoperability and the regulations adopted by the EU that are mainly addressing and focussing on the cross-border data exchange ecosystem. This section is addressing the legal interoperability which, as described in the EIF, is about ensuring that the public administrations are able to interconnect and work together under different legal frameworks, policies and strategies (European Commission, 2017). The following regulations enable mainly the legal and technical interoperability among the MS by requiring to collaborate and enable interoperability at all levels.

One of the milestones for achieving interoperable cross-border digital public services is the adoption of the eIDAS Regulation in 2014 (Regulation (EU) No 910/2014 of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, 2014). This Regulation aims to improve trust in electronic transactions by providing a foundation for secure digital interaction between public authorities, citizens and businesses. One of the main objectives of the eIDAS is to improve trust among the stakeholders and remove barriers in the cross-border use of national electronic identification by providing a framework for interoperable recognition of the national identifications in cross-border settings. However, this Regulation does not aim to intervene in the national electronic identification management systems and related infrastructures. In cross-border data exchange systems, one of the key building blocks is electronic identification and authentication. Not being able to securely identify and authenticate citizens across borders will hinder the achievement of seamless cross-border digital public services. Furthermore, the eIDAS Regulation also sets up the framework for electronic registered delivery service (ERDS), which is essentially the data exchange IT system

Draft

that enables the transfer of data and provides proof of evidence that data is transmitted. Recognition of the legal validity for the data sent through ERDS is also provided in eIDAS. However, there is no implementing act for ERDS adopted yet, which means that standards for ERDS are still unclear (Stasis & Demiri, 2017, p. 215). The recognition of eID and electronic delivery services are one of the reasons why the eIDAS Regulation is of huge importance for successful cross-border data exchange among public administrations in the EU.

Following the recommendations addressed in the EU resolutions and policy initiatives, the EU has adopted the resolution on Single Digital Gateway in 2018 (Single Digital Gateway 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, 2018). One of the main priorities addressed in the eGovernment Action plan 2016-2020 was the creation of the Single Digital Gateway for the citizens and business in the EU. The SDG regulation aims to create one single gateway in which the citizens and business would be able to get information, give feedback and to access online public procedures. It is important to be mentioned that the EC would not create a new portal, but rather an EU portal Your Europe will act as a single contact point to existing national portals (Akkaya & Krcmar, 2018, p. 158). In this Regulation, it is requested that all MS should enable fully online access to 21 procedures to the cross-border users. These procedures are related to the life events such as Birth, Residence, Working, Studying, Moving, Retiring and Starting, running and closing a business. One of the important goals of SDGR, inter alia, is to facilitate the use of these online procedures in line with the OOP in line with the safe and secure technical system. Article 14, more specifically of the SDGR, mentions that the MS should integrate the fully operational technical system to enable access for procedures for the cross-border users. It is also mentioned that this technical system should be secure and used only for the requested procedure. While technical and operational specifications of this technical system will be adopted by 12 June 2021.

To achieve the goals of the Single Digital Gateway, it is crucial to overcome the existing barriers of the cross-border exchange ecosystem in the EU, which will be further discussed in the next section.

Besides the enablers and drivers of the implementation of the OOP, there are several factors hindering the process of OOP implementation in cross-border settings. Mainly, research has shown that the MS are mostly concerned about the privacy and data protection issues, the legality of the data sharing across-borders, procedural differences, lack of political and managerial support and lack of financial support (Kalvet et al., 2018). Furthermore, the existing governmental silos and lack of organisational interoperability and alignment, also the organisational culture hinders the process of the OOP implementation in the cross-border setting (Krimmer et al., 2018, p. 3). Technological heterogeneity and maturity of the e-government systems are perceived by many authors and MS as the main barrier for the cross-border implementation of the OOP (Cave et al. 2017, Krimmer, Wimmer). Moreover, Mamrot and Rzyszczak (2020) state that the fragmentation of the OOP applications in the MS has a negative impact on extending EU-wide OOP (Mamrot & Rzyszczak, 2020). Similarly, Cave (2017) stated that the local solutions that are implemented in national borders are not designed for the cross-border data exchange while at the same time they so embedded, and the changes will be resisted (Cave et al., 2017). This has been proven by the research of Krimmer et al. (2018), in which it is found that the MS are not willing to undertake major changes to their legacy systems for cross-border reasons (Krimmer et al., 2018). The lack of technical interoperability can be seen in, inter alia, in the heterogeneity of the data exchange infrastructure systems, different approaches to handling data, access to distributed data sources. More specifically, due to the heterogeneity of the data-exchange infrastructures in the EU, it is difficult to achieve cross-border interconnection between local databases, and the solution needs to ensure a high degree of compatibility with the existing technological systems (Kalvet et al., 2018). In addition, one of the major challenges in the implementation of the OOP at the cross-border level is the mutual trust between the public administration on the cross-border level (Fedko, 2020). Similarly, citizens in the DACH region are also concerned about the seamless data exchange across borders, where two-thirds of respondents are having a negative impression of cross-border OOP (Akkaya & Krcmar, 2018).

Draft

To summarise, the main barriers for the EU-wide cross-border implementation, inter alia, are the heterogeneity of the data exchange infrastructures, existing legacy systems and willingness to undertake major technological changes for the sake of enabling it on the cross-border level. Several authors address these barriers by stating that MS should re-use already developed cross-border solutions such as CEF eDelivery (Wimmer et al., 2020) (Krimmer et al., 2018). Furthermore, lack of interoperability can be solved by following and adopting the solutions created by ISA^2 and by designing interoperable public services following recommendations, principles and interoperability model suggested by the EIF.

4.4 Organisational interoperability

4.4.1 Literature review

This section discusses the literature review of the drivers, benefits, enablers and barriers of the OOP and the cross-border data exchange systems in the EU. The literature review and the desk research has been conducted by using the search terms such as "cross-border data exchange", "data exchange systems", "cross border", "cross-sector data exchange", "intergovernmental data exchange", "electronic document exchange", "cross border data interoperability". The databases used for these purposes were Scopus, Google Scholar, Web of Science and Digital Government Reference Library. However, due to the increasing but still scarce and limited research on the cross border government data exchange, the data collection and analysis require further research on this topic (Krimmer et al., 2018; Wimmer et al., 2020). Following the EIF interoperability model, the main focus in this section is on organisational interoperability through which will be explained the cross-border exchange ecosystem in the EU. Organisational interoperability is described as “documenting and integrating or aligning business processes, and relevant information exchanged” (European Commission, 2017, p. 24).

Data exchange infrastructure governance in the MS and in the EU is one of the key criteria to achieve interoperable cross-border digital public services and a Single Digital Gateway (Wimmer et al., 2020). Data exchange infrastructures are defined as “*the whole of standards, technical components, services and governance framework in place for data exchange”,* and they are very important for the successful delivery of e-government services (Bharosa et al., 2020). Wimmer et al. (2020) and Rashid (2020) mentioned that data exchange infrastructures and identity mechanisms are key building blocks of the interoperability of different database systems (Rashid 2020), therefore, very important for achieving the OOP.

Achieving the OOP is one of the priorities in the Single Digital Gateway. Understanding of the OOP varies, in some countries, for instance in Estonia, it means that all data needs to be stored in only one database, while in France, it means that citizens and business need to provide personal data only once, which is also meaning in the EU policies and initiatives (Krimmer et al. 2017). Moreover, it is important to mention that Rashid (2020) differentiates two approaches to the adoption of the once-only policy, once-only as a principle and once-only as a programme. The main differentiation of these approaches is that adoption of the OOP approach addresses the changes in the whole government and possible transformation of the whole legacy system. While the once-only programme approach addresses the specific use case in the government (Rashid 2020). However, in this section, the main focus will be on the OOP approach due to the fact that the EU addresses achieving OOP in all policy areas.

The reason why the OOP is accepted as a priority in the EU policies on digital government transformation lies in the promise that it will reduce the burden on citizens, businesses, and public administrations when it comes to provision and collection of data (Halmos, Krimmer, Wimmer, Cave). Mainly, many authors are agreeing on that implementing OOP will bring various benefits for public administrations, business and citizens (Halmos, 2018; Krimmer et al., 2018; Krimmer et al., 2017; Rashid, 2020; Wimmer & Marinov, 2018). The benefits for public administration can be time savings, costs savings, higher administrative gains, increased efficiency and effectiveness, proactive public services, and the creation of better public services (Halmos, 2018; Kalvet et al., 2017). Last but not least, it is also considered that the “implementation of the OOP may lead to process optimisation in

Draft

governments and remove the duplication of some tasks." (Kalvet et al., 2017). Similarly, implementation of OOP in the government brings positive outcomes also to the citizens and business, mainly in time savings, reduced administrative burden, less cumbersome and more convenient procedures, increased transparency of the use of resources by the state (Wimmer & Marinov, 2018, p. 3). Finally, it is estimated that the implementation of the OOP in cross-border settings can increase cost savings up to 5 million euros (Cave et al., 2017; Halmos, 2018). However, although OOP brings various benefits to stakeholders in the public services creation, it is still poorly understood, as Krimmer et al. (2018) state, most likely due to the novelty of the concept and lack of cross border OOP initiatives.

The drivers for the implementation of OOP are mostly generated by the external triggers, such as in the demand of the citizens and business for reduced administrative burden, in the legal obligation (e.g. SDGR), or in improved service quality and better governance (Cave et al., 2017; Krimmer et al., 2018, 2017). Moreover, Krimmer et al. (2018) note that the participation in cross-organisational and cross-border knowledge transfer with strong leadership by the managers can be seen as a driver at the organisational level for the implementation of the OOP. Also, it is found that the maturity of the technical infrastructure and the existence of the OOP in the country can be seen as a driver for the implementation at the cross-border level (Krimmer et al., 2017). This shows that the difference in the maturity levels of the e-government and its data exchange infrastructures within the MS might have various effects on the adoption of the Single Digital Gateway. In addition to the drivers, to implement the OOP across the borders, several enabling conditions that are mostly internal triggers are needed to be considered. For instance, the main building blocks of the OOP are the electronic identification mechanisms and networked data exchange infrastructures, as well as the existence of the common standards and terminology for data exchange, in addition to the interoperability of the base registries (Krimmer et al., 2017; Wimmer & Marinov, 2018).

Besides the enablers and drivers of the implementation of the OOP, there are several factors hindering the process of OOP implementation in cross-border settings. Mainly, research has shown that the MS are mostly concerned about the privacy and data protection issues, the legality of the data sharing across-borders, procedural differences, lack of political and managerial support and lack of financial support (Krimmer et al., 2018, pp. 4–5). Furthermore, the existing governmental silos and lack of organisational interoperability and alignment, also the organisational culture hinders the process of the OOP implementation in the cross-border setting (Krimmer et al., 2018, p. 3). Technological heterogeneity and maturity of the e-government systems are perceived by many authors and MS as the main barrier for the cross-border implementation of the OOP (Cave et al. 2017, Krimmer, Wimmer). Moreover, Mamrot & Rzyszczak (2020) state that the fragmentation of the OOP applications in the MS has a negative impact on extending EU-wide OOP (Mamrot & Rzyszczak, 2020). Similarly, Cave (2017) stated that the local solutions that are implemented in national borders are not designed for the cross-border data exchange while at the same time they so embedded, and the changes will be resisted (Cave et al., 2017). This has been proven by the research of Krimmer et al. (2018), in which it is found that the MS are not willing to undertake major changes to their legacy systems for cross-border reasons. The lack of technical interoperability can be seen in, inter alia, in the heterogeneity of the data exchange infrastructure systems, different approaches to handling data, access to distributed data sources. More specifically, due to the heterogeneity of the data-exchange infrastructures in the EU, it is difficult to achieve cross-border interconnection between local databases, and the solution needs to ensure a high degree of compatibility with the existing technological systems (Kalvet et al., 2017). In addition, one of the major challenges in the implementation of the OOP at the cross-border level is the mutual trust between the public administration on the cross-border level (Fedko, 2020). Similarly, citizens in the DACH region are also concerned about the seamless data exchange across borders, where two-thirds of respondents are having a negative impression of cross-border OOP (Akkaya & Krcmar, 2018).

To summarise, the main barriers for the EU-wide cross-border implementation, inter alia, are the heterogeneity of the data exchange infrastructures, existing legacy systems and willingness to undertake major technological changes for the sake of enabling it on the cross-border level. Several authors address these barriers by stating that MS should re-use already developed cross-border

Draft

solutions such as CEF eDelivery (Krimmer et al., 2018; Wimmer et al., 2020). Furthermore, lack of interoperability can be solved by following and adopting the solutions created by ISA[2] and by designing interoperable public services following recommendations, principles and interoperability model suggested by the EIF.

4.4.2 National approaches

The heterogeneity of the data-exchange solutions within the EU can be presented by describing solutions that the several EU MS are using. As already explained, the heterogeneity of the data-exchange infrastructure and also the legacy systems are considered a major barrier to the development of the Single Digital Gateway. This section shortly describes some of the national solutions MS are using for the data exchange between national public administrations. The selection of countries in this analysis is based on the participation on the large scale projects in the once-only principle.

One of the pioneers in the digital transformation in government is Estonia, also considered as the leading country in the digitalisation of public services. This high development in digital transformation can be prescribed to their data exchange system X-Road. This secure exchange internet-based communication protocol is considered as a backbone of the OOP in Estonia because it enables the connection between multiple databases and enables data sharing among them (Mamrot & Rzyszczak, 2020). During the phase of the creation of the system, the aim of this data-exchange system was not to replicate existing data in database systems but rather to re-use and connect different database systems to communicate and to enable the secure sharing of data (Cave et al., 2017). The main characteristics of the X-Road, inter alia, are that it is open-source, autonomous, confidential, interoperable and secure (Rashid, 2020). Next to the X-Road system, it is important to mention that Estonia has a mature and high degree of uses of its eID solution, which enables the implementation of the OOP. Also, other countries are using the X-Road solution, such as Finland, which uses the X-Road solution for their data-exchange purposes. Consequently, Estonia and Finland are also the pioneers in the cross-border implementation of OOP. With the bilateral agreement and connection of the Finland databases in the central server of X-Road, data stored in databases in both countries are shared by utilising the X-Road system (Akkaya & Krcmar, 2018). It is very important to mention that X-Road is centrally governed and that it is used by all public administrations for all kinds of data exchanges, while it also allows uses by private parties (Bharosa et al., 2020).

The Netherlands, however, is using multiple data exchange systems to enable the implementation of the OOP. This is the reason because the institutional structure requires a demarcation between private and public infrastructures (Bharosa et al., 2020, p. 41). These systems are Digikoppeling, Digilevering, Digimelding, and Stelselcatalogus, and they are employed in order to enable seamless data exchange between public administrations. The Netherlands also have a system of agreements for data exchange systems, Diginetwerk, which includes multiple networks and databases by employing the above-mentioned systems.

In Austria, the implementation of the OOP is enabled by its data exchange system Register and System Network (RSV) (Fedko, 2020). This data exchange system interconnects 130 databases of the various public administrations, and it acts as an interconnector between the databases and front-end solutions. RSV is considered a prerequisite for OOP implementation by the Austrian authorities because it facilitates the exchange of data in a transparent and secure environment.

Slovenia, instead, similarly to the Netherlands, use different systems to implement OOP. Three main building blocks for data-exchange are Tray, IO module and Asynchronous Module. These building blocks were developed primarily for the e-social security data exchange, but it is also used for other purposes (SCOOP4C). Slovenia has developed a central system for electronic delivery, SI-CeV, which enables the secure exchange of documents between public administrations, citizens and businesses (NIO, 2021). This system can also be used for cross-border connection and implementation of the cross-border OOP.

Belgium, as a federal state, uses different exchange systems at the federal and state level. For instance, the Flemish government uses the MAGDA (Maximum Data Sharing between

Draft

Administration and Agencies) platform to enable data exchange between 190 agencies and 13 departments of the Flemish government and 308 local governments (Kalvet et al., 2017). On the federal level, Belgium utilises Federal Service Bus to enable data exchange between different public administrations and multiple ministries. Federal Service Bus is also used for cross-border purposes and acts as a cross-border connector that allows access to the national registries while taking into consideration security and data protection principles (Fedko, 2020).

Finally, these different national solutions for data exchange purposes shows that the development of the solutions was undertaken mostly for national purposes. In addition to the technical differences, the additional difference among these solutions is also based on the governance and control of these solutions. For instance, some countries have centralised data exchange solutions (such as Estonia and Slovenia), while in some countries, there are multiple solutions for the data exchange (such as the Netherlands).

4.4.3 National and cross-border data exchange approaches

Rashid (2020) describes three possible approaches for data exchange at the national level. Data-exchange systems at the national level could be designed as a centralised model, distributed model or federated model. In the centralised approach of the data exchange systems, all data is stored under one single data authority, through which other parties need to make a direct request for access. Under this model, the benefit is that it offers efficiency and transparency; however, the technological system in the centralised model needs to be secure and reliable in cases of emergencies. It is important to mention that this model is hardly used at a federal or governmental level. Conversely, under a distributed approach, every public administration has its own database of resident data. Due to the fact that every administration has its own database, the data exchange system is not an integral part of the infrastructure, and thus it needs to be additionally created. Since this approach is consisted of multiple databases, it requires careful design of the digital service and infrastructure to enable interoperability to achieve seamless data exchange, thus the OOP. The federated approach can be considered as a mix of the centralised and distributed approaches. In the federated approach, public administrations collect only relevant data for their purposes, while additional data is collected from the administrations. To exchange the data within the federated approach, a centralised data exchange infrastructure is required, which will enable the data exchange between the administrations. According to Rashid (2020) the best approach for implementing OOP is the federated approach because it enables the connection to one centralised data exchange system within the distributed databases (Rashid, 2020).

While having this heterogenous digital environment in the EU, there are several possibilities for cross-border cooperation. Aavik & Krimmer (2016) classify four different possibilities for cross-border cooperation using the Estonian case (Aavik & Krimmer, 2016). Forming bilateral agreements between MS is one of the options, which can be utilised the already existing national data exchange infrastructure. An example of a bilateral agreement is the already mentioned cooperation between Finland and Estonia. The second option is the creation of e-residency rights by giving an opportunity to non-Estonian citizens to have business rights and to conduct business in Estonia with also providing a unique identifier through eID. The third option for the cross-border cooperation is the non-governmental body involvement, mostly likely private actors acting as intermediary providing secure and trusted services. An example of this option can be SingWise which provides digital identification services for cross-border purposes. Last but not least, Aavik and Krimmer (2016) explain the fourth possibility of creating a supranational framework, in which transnational interference is considered as the most effective and efficient solution. An example of the technical solution created to follow the supranational framework possibility are the building blocks of CEF, eID and eDelivery solutions.

The explained approaches of the data-exchange systems are not only applicable on the national level but can also be considered on the cross-border level. Possible collaboration for data-exchange on the cross-border level can be bilateral agreements, multilateral agreements and supranational (federated) agreement. The bilateral agreement requires two MS to enable the data-exchange between their public administrations by employing centralised data exchange infrastructure. An example of a bilateral agreement of cross-border data exchange is an agreement between Finland

Draft

and Estonia, in which both countries are connected to the X-Road server. The multilateral agreement requires the interconnection of MS public administrations within one agreed data-exchange system, thus enabling peer-to-peer direct data exchange of relevant parties. Finally, supranational or federated agreement requires the MS and associated countries, to connect to one data-exchange system and thus enable data-exchange across borders in an interoperable way. The interconnection of all countries within this federated approach could enable interoperability of the different IT systems and possibly overcome the technical interoperability barriers caused by different IT infrastructures within the EU.

Finally, as already mentioned, the Single Digital Gateway regulation requires that all MS and associated countries offer access to fully online procedures by also cross-border users through Your Europe portal. Having multiple agreements between the MS and also bilateral agreements might create many interconnection points and networks, which might further deepen the heterogeneity of IT systems within the EU. Thus, the best option to enable cross-border data-exchange could be through a data-exchange connector which will enable the interconnection of different IT infrastructure public administrations. Therefore, the best cross-border agreement would be a federated approach by re-using the already developed cross-border solution of CEF eDelivery, which will be described in the next subsection.

4.5 Cross-border solutions

Currently, there are several solutions for data exchange on the cross-border level. These solutions are mostly initiated by the European Commission as the leading institution in enabling cross border interoperability.

4.5.1 eDelivery

The eDelivery is a building block that enables the secure communication and exchange of data between public administration, business and citizens on the cross-border level ((Joinup, 2021)). The motivation for the development of this solution is the existing heterogeneity of the IT infrastructures within the MS and the necessity to create a secure interoperability layer that will interconnect these heterogeneous systems (CEF eDelivery, 2015). The eDelivery solution helps public administrations to exchange data by providing the technical specifications and standards which enable every user to become a node in the network. This distributed model of the eDelivery building block enables direct communication between the users without setting up a new bilateral channel. eDelivery enables public administrations to exchange data and documents not only with other public administrations but also with business and citizens. This solution can be used not only in the cross-border environment by connecting different IT systems of MS but also in the national and regional environment by connecting different IT systems within the country.

The eDelivery is based on the four-corner model, as can be seen in Figure 4. This means that the data or documents pass through four layers - the backend of the sender (C1), the senders' Access Point (C2), the receiver Access Point (C3) and the backend of the receiver (C4). The communication between these layers is enabled by the AS4 messaging protocol. These Access Points are the nodes that enable the technical interoperability between the heterogeneous IT systems in the EU.

Draft

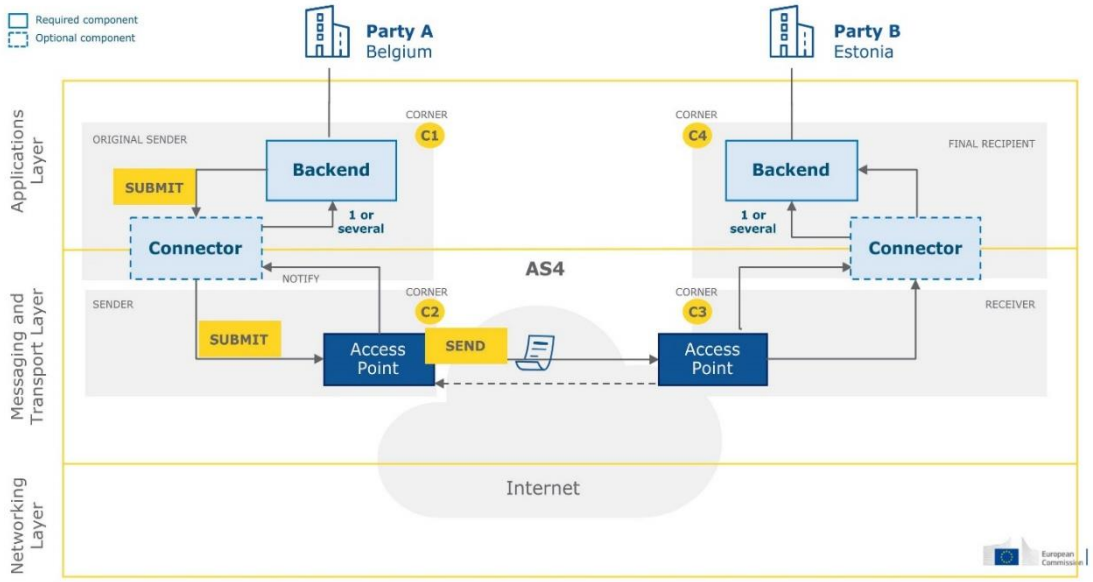

Figure 4: eDelivery 4 step model (Rodrigues Frade, 2016)

The use of the eDelivery solution can bring several benefits such as, inter alia, savings in the cost of creating, maintaining and operating data exchange networks, fostering synergies of service providers (CEF eDelivery, 2015). Finally, it is important to mention that there are several eDelivery Access points per the MS, each assigned to a specific policy domain such as eProcurement or eJustice.

4.5.2 BRIS

Another relevant EU initiative that enables cross-border data exchange between the MS is the Business Registers Interconnection System (BRIS). The BRIS infrastructure provides a cooperation platform for all European Business Registers. It provides to the citizens, business and public administrations a single point of access on the eJustice platform, on which they can search and find the relevant information on companies and their branches (Kalvet et al., 2017). The purpose of the BRIS infrastructure is to improve cross-border access to business information is achieved by enabling communication between business registries. BRIS is using a public network in order to enable access to citizens business and public administrations to find a piece of information. The system is distributed with a central component of storing and indexing the published information (European Commission, 2019). To enable secure and reliable data exchange, BRIS uses CEF eDelivery building block. Finally, the benefits of BRIS are that it reduces administrative burden, increases consumer confidence, increases legal certainty and efficiency of procedures (Kalvet et al., 2017).

4.5.3 EESSI

The Electronic Exchange of Social Security Information System (EESSI) is the IT platform that enables data exchange by social security institutions across borders. Most exchanges between public administrations related, inter alia, to sickness, occupational disease and accidents at work, pension, unemployment, were paper-based which was being replaced by the electronic data exchanges by the rollout of EESSI (European Commission, 2021).The first data exchange related to the social security of EU citizen took place in 2019, and since 2019 all EEA MS are required to connect to the system. To exchange the information, EESSI uses a private network, and it has a routing component that enables the secure and reliable exchange of information. Use of EESSI benefits public administrations but also to citizens by enabling: Faster and more efficient information exchange, more accurate data exchange, safe IT environment for data exchange, secure handling of personal data and verification of social security rights. By 2022 it is expected that more than 15 thousand social security institutions in 32 countries are able to fully exchange information across borders.

Draft

4.5.4 EUCARIS

The European Car and Driving Licence Information System is a decentralised IT system that connects the MS, which enables the sharing of information related to vehicle and driving licence and other transport-related data (EUCARIS, 2021). EUCARIS is an exchange mechanism and not a database nor a central repository, and it is developed in order to reduce car theft and registration fraud within the EU. The value of EUCARIS is that it enables the cross-border data exchange within the transport and mobility sector by enabling a peer-to-peer connection between the MS. Also, the goal of EUCARIS is to avoid the creation of the new system for data exchange every time when a new agreement, treaty or directive comes into force. By having one exchange information system, it achieves costs and time savings and higher interoperability (EUCARIS Secretariat, 2020).

4.5.5 OpenPeppol

PEPPOL is a set of artefacts that enables the cross-border interconnection of eProcurement systems through loosely coupled building blocks. The PEPPOL network uses the eDelivery Access Point to enable the interconnection between multiple parties in the EU. This solution provides technical specification and open-source software for data exchange related to the eProcurement phases by enabling the communication between heterogeneous data exchange infrastructures. Exchange of information, similarly to the eDelivery building block, is enabled through the four-corner model and access Points acting as interoperable nodes (Figure 5). This enables a many-to-many interoperability environment, and it reduces costs and burden on creating bilateral agreements and the creation of new systems (PEPPOL, 2016).

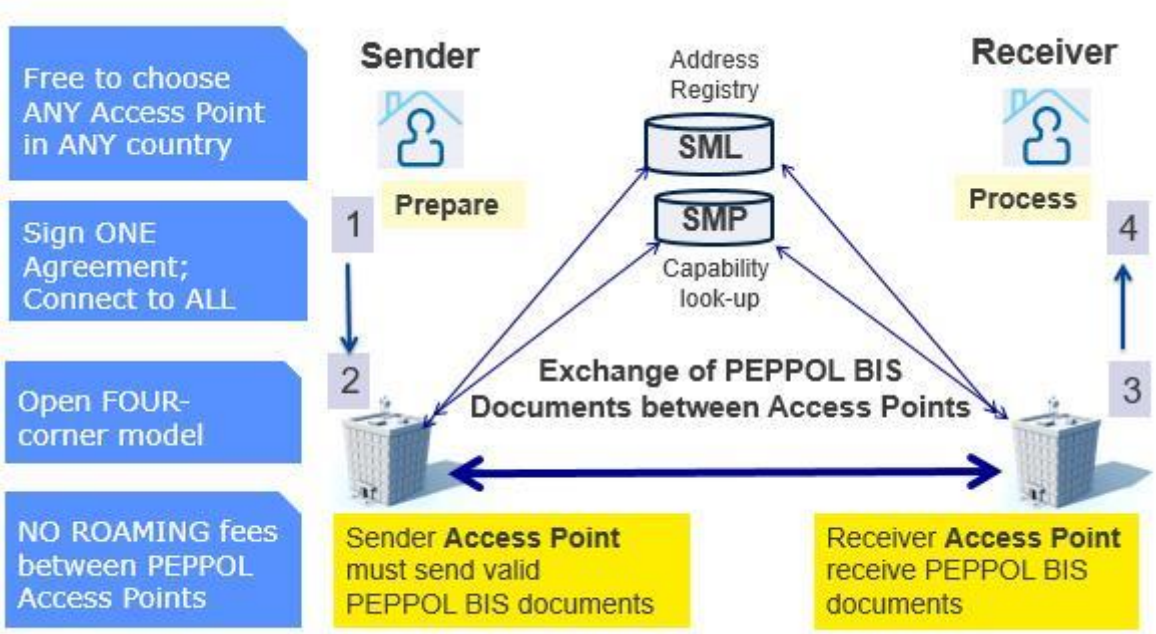

Figure 5: PEPPOL eDelivery network (OpenPEPPOL, 2021)

4.5.6 TOOP Solution

The OOP solution created by the “The Once-Only Principle” (TOOP) project will be further discussed and analysed in the next section on technical and semantic interoperability. TOOP architecture proved the feasibility of achieving a OOP in a cross-border setting, and therefore having SDGR as a basis of the creation is the best example to explain the technical and semantic interoperability of federated data-exchange architecture.

4.6 Semantic interoperability

4.6.1 TOOP architecture/approach

Starting from the once-only-principle and integrating some of the most important EIF recommendations related to re-usability, interoperability, security, and privacy, the architecture of the TOOP project defined for the Information System (IS) Architecture two main layers: the TOOP connector and the eID Component, integrating with the Digital Service Infrastructure (DSI) Building Blocks (BB) for some of the services like eDelivery, eSignature, eDocument, eTranslation, Trust Management and Semantics (see Figure 6).

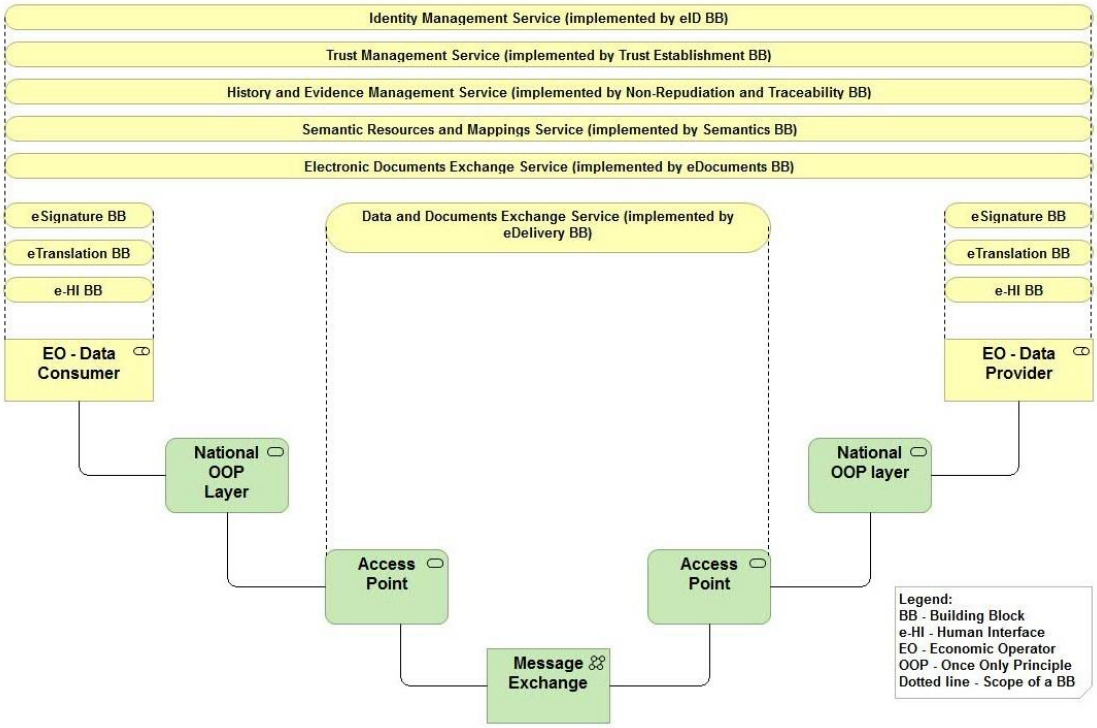

Figure 6: TOOP architecture building blocks (BB) (source D2.1 of TOOP Project)

Regarding Data Quality and more specifically the data accuracy, the semantic modules play an important role in the data exchange. The semantic interoperability view specifies only one process, the **semantic mediation** and the TOOP project attempted/proposed a loosely coupled semantic architecture, as the monolithic approach is hindering the OOP.

Based on the diagram from Figure 7, there have been three semantic building blocks defined: one for semantic mapping, matching and mediation service, a second one for the base registry service to store authentic data and a third one for the alignment governance, registry and discovery service.

The semantic mediation service was designed to be used in on the Data Consumer (DC) side for evidence identification, as well as evidence interpretation and on the Data Provider (DP) for evidence extraction (TOOP, 2018).

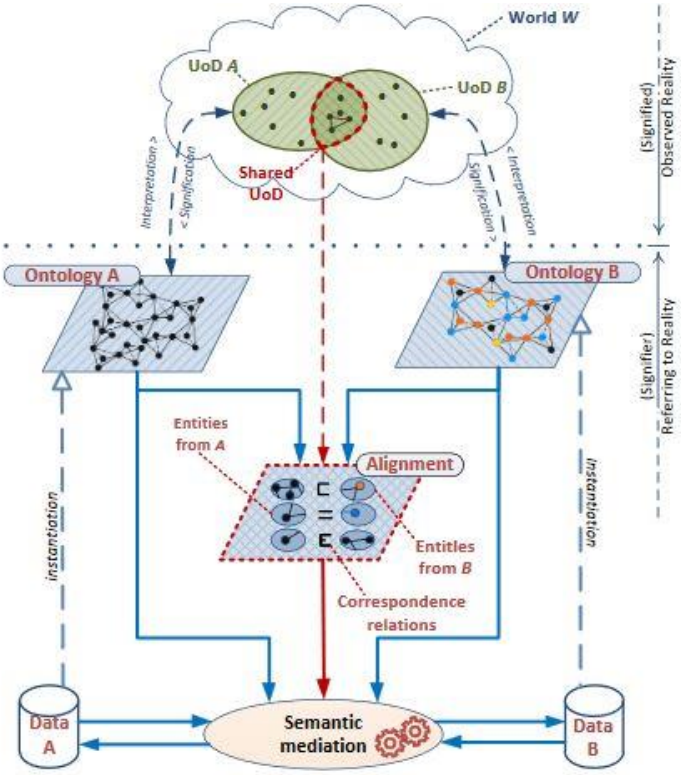

Figure 7: Semantic interoperability view (source D2.1 of TOOP Project)

As founding aspects of the semantic view, the ontology handling components have been designed as follows:

- an **OOP Semantic Model** that describes entities relevant when the OOP is applied. These entities are generic and not affected by the domain the architecture is applied to, taking also the SDGR regulation into consideration. This comprises the following reused ISA^2 core vocabularies concepts and their relation: Natural Person, Legal Person, User, Competent Authority and Evidence. Some other concepts still need to be defined.
- a **methodology for modelling Domain Semantic Models** based on the methodology proposed by ISA^2 "e-Government Core Vocabularies handbook" and the SDGR regulation. The methodology comprises of the phases: specification, information modelling, business rules, implementation, documentation and evaluation. At this phase, the conceptual model is transformed into a computable model (XSD, Schematron file, RDFs), using a representation format (XML Schema, RDF, OWL)

Regarding the implementation in the area of semantics, the design on how Core Vocabularies from the ISA^2 program were intertwined with Application Profiles in the TOOP architecture is described on the project wiki page (TOOP, 2020a).

The extended set of Core Vocabularies are implemented in the semantic data models of the central components like the Data Services Directory (DSD), the Criterion & Evidence Type Rule Base (CERB) and the TOOP Exchange Data Model (EDM), with the goal to achieve **horizontal, cross-service and cross-actor semantic interoperability**. An overview on how the models are used in the TOOP services and components is detailed at (TOOP, 2020e).

4.6.2 DE4A

Digital Europe for All (DE4A) is a project started on the 1st of January 2020 (DE4A, 2020). The project is planned to be built upon the existing infrastructure, it attempts to contribute to an overarching eGovernment network for Europe supporting parallel efforts from the EC and the MS to realise the OOP Technical System in compliance with Single Digital Gateway and aligned with EU eGovernment Action Plan 2016-2020, Tallinn Declaration and EIF Implementation Strategy. Therefore, the reuse of existing technical building block prepared by previous projects like e.g. TOOP Citizen and provided

Draft

by CEF is expected. Business-oriented pilots shall highlight chosen aspects of the technical ecosystem available for the SDG implementation on the European and MS level.

A specific focus will be put on assessing the applicability, benefits and cost effectiveness of innovative technologies with transformative impact: blockchain (for effective disintermediation and notarization, fostering accountability and transparency in distributed transactional environment) and machine learning (over usage data to automate monitoring and improve effectiveness / quality of SDG-related procedures).

4.6.3 eHealth services

Semantic interoperability in eHealth Services plays a very important role in the data exchange of information. One of the communication standards, HL7, has been upgraded in the last years with a data model that allows REST operations and semantic interoperability of patient health record by introducing the HL7 Fast Healthcare Interoperable Resources (FHIR) framework. The initiatives and projects where it is employed range from International Patient Summary (IPS) (HL7 International, 2020, p. 7), clinical studies data storage and processing (Leroux, 2017) to bioresearch apps (Carolina, 2017).

Regarding the semantics of the exchanged data, a set of Service-oriented Architecture (SOA) based Common Terminology Services were defined by the HL7 standardization organization (HL7 International, 2020, p. 7).

As an example, a set of common used semantic resources include those describing the allowed values ValueSets and ConceptMaps, bearing associated metadata referencing CodeSystems like LOINC or SNOMED and possible display text, often with information regarding the used language. Thus, services like **retrieving the appropriate value** from the ConceptMap for encoding purposes, **validation of used value** and **display in different languages** is possible.

The maturity of the FHIR standard has invited the EU eHealth Digital Service Infrastructure (eHDSI or eHealth DSI) to use it when defining the semantic service specification (EHDSI, 2020).

One of the implementations of the terminology services defined by HL7 FHIR is the CTS-LE server from Fraunhofer FOKUS (Fraunhofer FOKUS, 2021), that was successfully used and extended in EU projects like epSOS (Smart Open Services for European Patients) (European Commission, 2014).

4.7 Technical interoperability

4.7.1 TOOP architecture

As can be seen in Figure 8, a TOOP application uses the following components: communication networks in the MS, TOOP central communications infrastructure, the eIDAS network, and the Internet, see (TOOP, 2019).

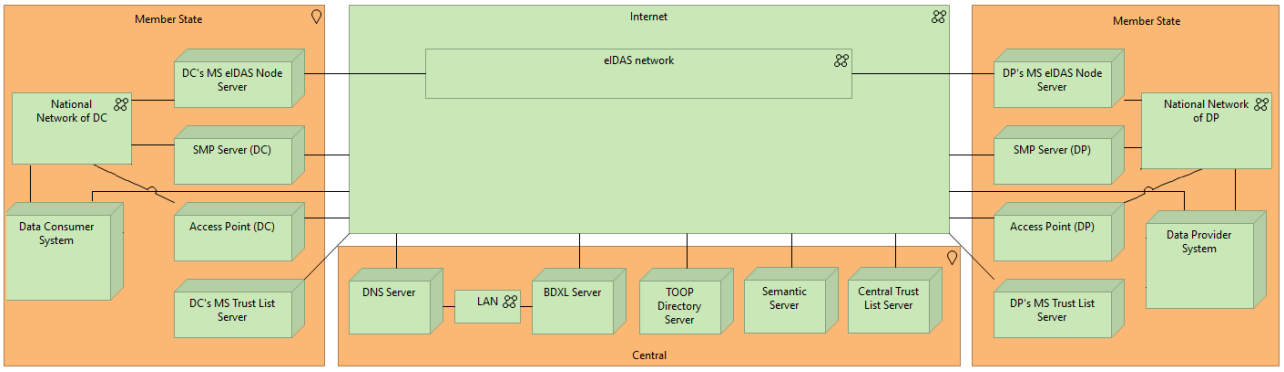

Figure 8: TOOP architecture

The eIDAS network is employed for user identification. The Service Metadata Publishing (SMP) (OASIS, 2021) server is used for communication endpoint discovery and the access point for

Draft

evidence exchange. The list of qualified trust service providers and the provided services are published on the MS trust list servers. The SMP endpoint registration to Service Metadata Location, now bearing the name of OASIS BDXL, is described at (TOOP, 2020c). At the base of the technical interoperability stays the CEF eDelivery solution based on a distributed model called the "4-corner model". In this model, the back-end systems of the users don't exchange data directly with each other but do this through Access Points. These Access Points support the same technical **OASIS AS4** specification and therefore capable of communicating with each other.

The project has also produced a deployment view of the technology architecture, having the presence of the National Network depending on the use case.

In terms of the components offered by the TOOP project, the conceptual architecture from Figure 9 offers more details. The central have the following functionality:

- **Criterion and Evidence Type Rule Base (CERB)** is a central authoritative system that maps specifics sets of Data as Evidence that prove specific requirements. The DC consults the CERB in order to find which type of Data (Dataset) can be requested as an evidence for a specific User, taking into account the User's country and/or jurisdiction. The DG GROW's eCertis is designed to act as CERB system for the TOOP project (TOOP, 2020b).
- **Data Services Directory (DSD)** is a central service that acts as a catalogue of Datasets that the DPs can provide upon request. It links specific DPs with Datasets, so that the DC can discover them and submit Evidence Requests.
- **Registry of Authorities (RoA)** is a core service that lists, for public administrations in EU MS, the procedures for which these administrations are authorized to request which types of evidence. The Registry of Authorities can complement and provide a context for, but is not a replacement of, the explicit request/input of the user. The component is part of the TOOP connector.
- **CEF eDelivery Common Services** represented by the **Service Metadata Publisher (SMP)** and **Business Document Metadata Service Location (BDXL)** services, based on OASIS standards, provide the metadata about the eDelivery access point(s) used by Data Consumers and Providers in the evidence exchange process. CEF eDelivery helps the actors to exchange electronic data and documents with one another in a reliable and trusted way.
- **TOOP Exchange Data Model (EDM)** provides a standards-based message model that is used to express uniformly the Evidence Requests and Responses.

Draft

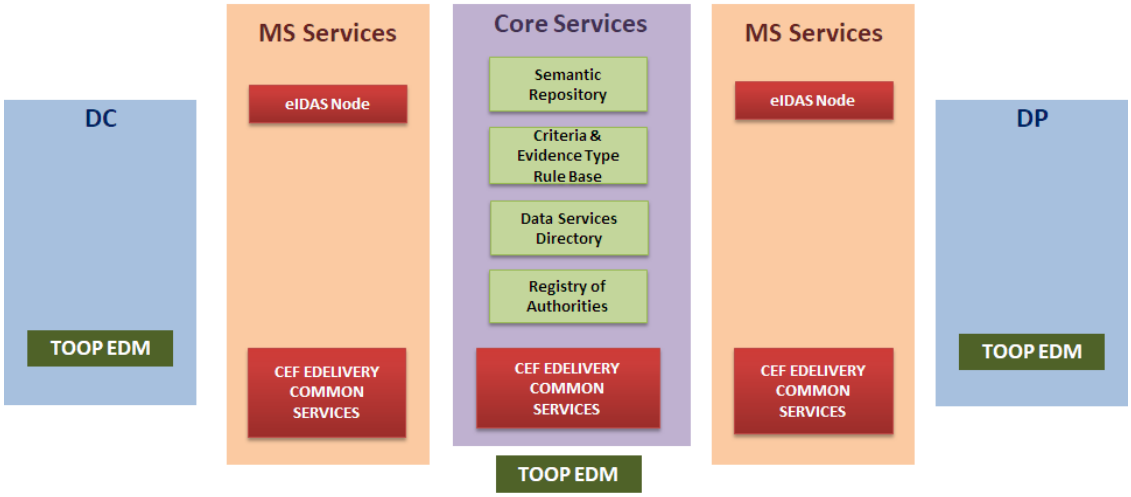

Figure 9: TOOP conceptual architecture

Taking a deeper look at the technical implementation, the project documentation (TOOP, 2020d) also offers a complete diagram of message flows considering that a user wants to execute a procedure provided by the Data Consumer (see Figure 10).

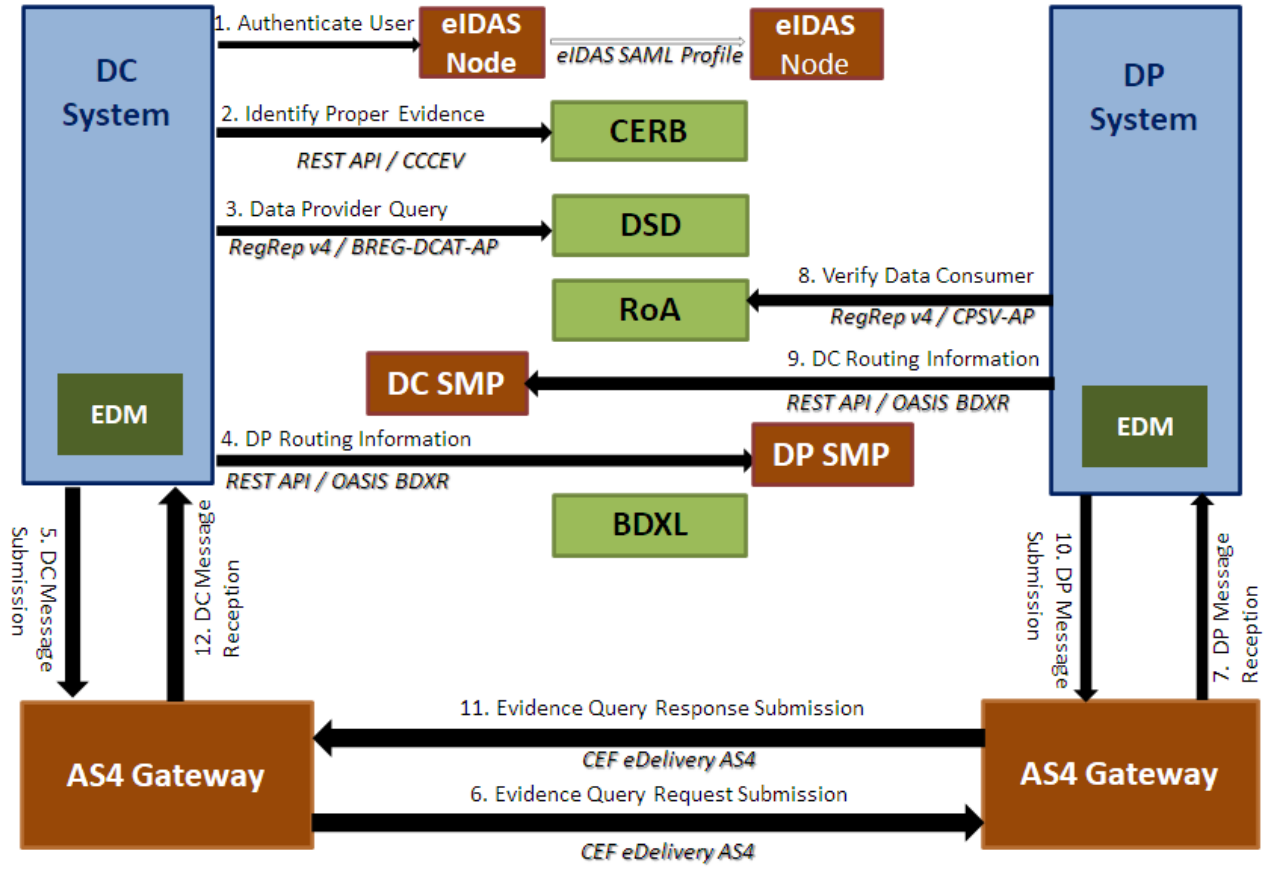

Figure 10: TOOP message flow

The TOOP-connector (TC) software component, encompassing the toop-edm component, contains both a plugin for an external AS4 Gateway as well as built in AS4 Gateway that has connections to the PEPPOL and e-SENS version of the component (Helger, 2021).

The DSD service uses by default its own publicly available instance of a Peppol directory (TOOP, 2021) from which it pulls the data about available services.

Overall, the components from the TOOP project as well as the simulator that provides an easy approach in providing the components to the developers of the Data Consumer and Data Provider applications need to be practically assessed and validated. Based on the requirements and the reference architecture from D1.3 and D1.2, the decision on whether and how to reuse and adapt them will take place in WP2 and WP3.

4.7.2 Identity matching

The databases used by the different administrations in the MS are mostly designed for specific cases or services. The underlying structure of the register quite often are set up before generic rules to exchange eIDs like in the eIDAS regulation were established. The data schemes are strongly related to the provided services. This causes a gap of attributes that allows an automated exchange of information and mapping of identities. Different information is collected about citizens and businesses and may identify people and organisation differently. To make it even more difficult, some MS (e.g., Germany) do not have persistent identifiers or provide such persistent identifiers only as optional attributes. This causes a range of problems to match the identity of a legal or natural person already on a national but especially supranational level.

4.7.3 Record matching

Identification in Europe happens via eIDs notified under eIDAS. In this case, there is a record matching issue depending on MS infrastructure. While using notified eIDs under the eIDAS

Regulation for the most part will allow data providers to match an identity with a record (evidence requested) using the attributes of the natural person provided by the eIDAS minimum data set, in some cases additional attributes are needed to ensure a match. This is based on a lack of interoperability and the credentials defined in the eID schemes of the MS.

The lack of a match with the regulated electronic identity circuits falls under the national sovereignty, and the consequent lack of a sound legal basis.

4.7.4 eHealth services

During the project e-SENS, a sample implementation of an eIDAS Node assuring a Distributed Cross-border Authentication (DCA) was released under the name of e-SENS Authentication Broker. It already has support for on-boarding different domains like eHealth (European Commission, 2014) (European Commission, 2016) and thus, have **national eIDs used for eHealth could also be used on the eIDAS Network** (see also Figure 11). The next technical level of patient identification consists of using a virtual eID (mobile eID), as in the mGov4EU project.

Moreover, some of the health insurance cards are now electronic and store a PKI key-pair that allows through an exposed Near Field Communication (NFC) interface both authentication against an OpenID Connect identity management server as well as establishing a TLS communication between patient App and eHealth services, like the one from Germany (Corici et al., 2020). In addition, the European Health Insurance Card mapped to the national card can be used to access medical services with SHI accreditation.

For technical interoperability for **cross-border eHealth services for medical purposes**, including exchange of vaccination information in the **International Patient Summary**, the National Contact Points for eHealth in both the patient origin country and the country of the medical service can use the sample implementation from the epSOS project.

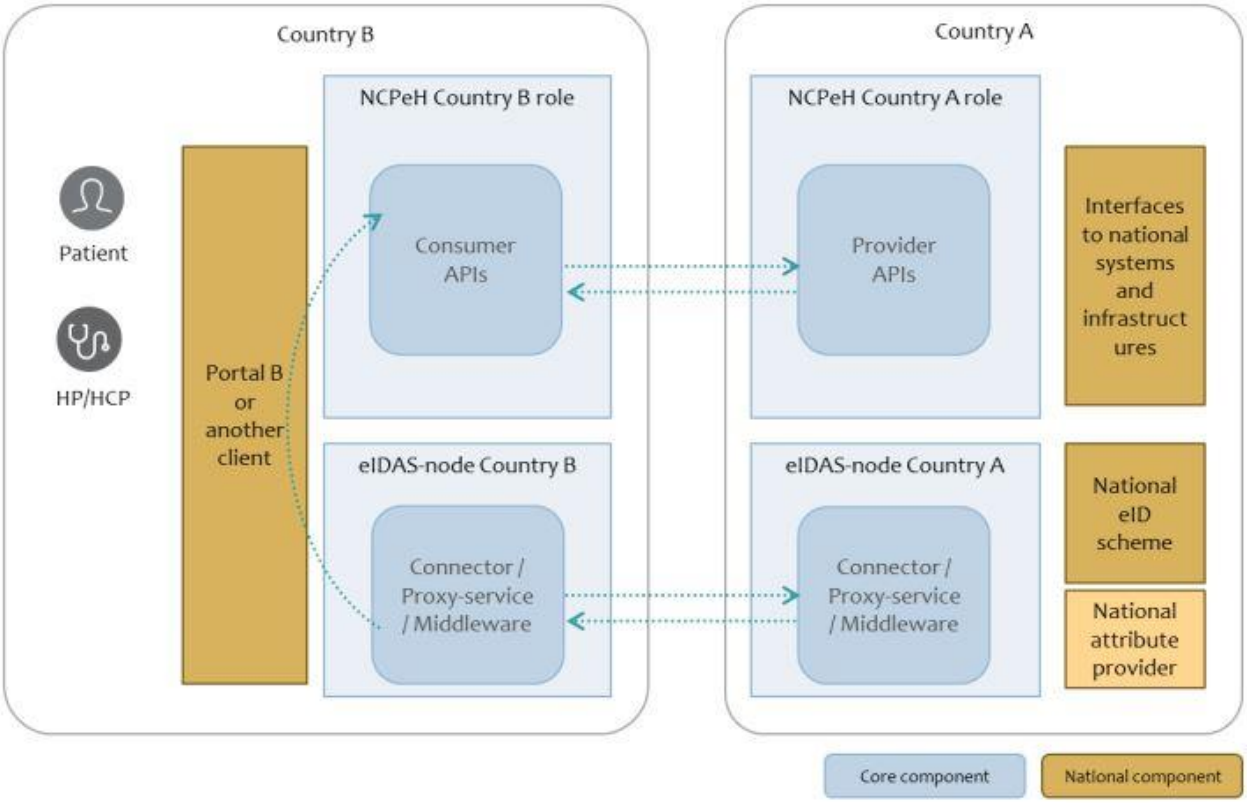

Figure 11: Basic setup for implementing eID for eHealth (European Commission, 2016)

4.8 Initiatives evaluation

Evaluation Matrix (Table 3) presents the collection of the cross-border solutions and the specifications criteria on the features of the cross-border solutions. Categories included in the Evaluation Matrix are:

- Public Access:
  - *Public Network* (the general public can access the solution and search for information) or
  - *Private Network* (only public administrations have access to the solution);
- The system distribution:
  - *Purely Distributed System* (the system is purely distributed when it enables peer-to-peer communication without a central platform or routing component) or
  - *Central Platform/Routing Component* (the system is connected to the routing component and/or central platform);
- Governance level:
  - *Centralised organisation* (the solution is maintained and administrated by one authority) or
  - *Decentralised organisation* (the solution is maintained and administrated by the users). The results of this evaluation matrix can be seen in Table 3.
- eIDAS compliance

Draft

Table 3: Evaluation matrix of the cross-border solutions

Evaluation Matrix	Public Access		System distribution		Governance level		eIDAS
	Public Network	Private Network	Purely Distributed System / No central platform	Central platform / Routing com-ponent	Centralised organisation	Decentra-lised organisation	eIDAS interface / com-pliance
BRIS	x			x	x		
EUCARIS		x	x			x	
EESSI		x		x	x		
TOOP		x		x	x		x
DE4A[18]		x		x	x		x
Open-Peppol		x		x		x	x

Draft

The heterogeneity of the solutions and the differences among them show that most of the solutions presented are sector specific. This implies that they mostly use the private networks with a federated distribution approach, with most solutions having a centralized governance level of the organisation. Furthermore, it can be seen that only EUCARIS, which is created by the initiative of the Member States is having different results in the evaluation compared to other EU initiated solutions.

[18] As the DE4A project is ongoing, the answers are preliminary and based on the information that are available at the time this deliverable was written.

Chapter 5 Summary and conclusion

The objective of this deliverable was to research related work and specifications on "*mobile eID, eDelivery, eGovernment and eGovernance*" (quoted from the mGov4EU DoA). The purpose was to set the scene to serve as a basis for adjacent architecture and development work. Thus, a primary goal was to survey what is most relevant to our project, namely related work that can be re-used in advancing processes related to the EU Single Digital Gateway Regulation and the EU eIDAS Regulation to mobile use cases. This initial technical work of mGov4EU, however, went a bit beyond by researching also approaches that do not necessarily origin from the EU, or solutions and standard that do not necessarily address mobile devices, while all still having some relation to the mGov4EU goals. The idea was to survey broader than originally considered to learn from approaches that, while might even being outside our comfort zone, could give further input to be considered when developing the architecture.

On eGovernment and eGovernance a thorough literature review was carried out. The research has been influenced by the Grounded Theory method and addresses key factors as drivers as quality, trust and security, awareness, attitude and image, user experience and perceived value, demographics, infrastructure, and provision, and, finally, mobile strength have been analysed.

The work in mobile eID also started with a literature review specifically addressing electronic identification. Following EIF layers, international policy frameworks on eID were analysed to compare to eIDAS. The survey on standards and specifications went broad, as it listed and summarized several initiatives on identity management, authentication, authorisation, self-sovereign identity, and mobile apps. This was followed by an overview of concrete eID solutions, both notified under eIDAS but also further European and international public-sector and private-sector solutions.

Like the other sections, the overview of cross-border data exchange includes a thorough literature review. Furthermore, it analyses relevant initiatives at all EIF layers on policy, legal, organisational, semantic, and technical interoperability. The initiatives that were analysed are the cross-border delivery aspects of the business registers interconnection system BRIS, the European car and driving license information system EUCARIS, the electronic exchange of social security information EESI, and the cross-border large scale pilots the once-only project TOOP, digital Europe for all DE4A, and Open-Peppol as successor of the pan-European public procurement online pilot PEPPOL.

To summarize, the deliverable gives a comprehensive view of related work on mobile eID, eDelivery, eGovernment and eGovernance. This shall serve as a knowledge base for the follow-up work in mGov4EU.

Draft

Chapter 6 Bibliography

Aavik, G., & Krimmer, R. (2016). Integrating Digital Migrants: Solutions for Cross-Border Identification from E-Residency to eIDAS. A Case Study from Estonia. In H. J. Scholl, O. Glassey, M. Janssen, B. Klievink, I. Lindgren, P. Parycek, E. Tambouris, M. A. Wimmer, T. Janowski, & D. Sá Soares (Eds.), *Electronic Government* (Vol. 9820, pp. 151–163). Springer International Publishing. https://doi.org/10.1007/978-3-319-44421-5_12

Abraham, A. (2017). *Whitepaper – Self-Sovereign Identity*. A-SIT. https://technology.a-sit.at/en/whitepaper-self-sovereign-identity

Abraham, A., Hörandner, F., Omolola, O., & Ramacher, S. (2020). Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems. In J. Zhou, X. Luo, Q. Shen, & Z. Xu (Eds.), *Information and Communications Security* (Vol. 11999, pp. 307–323). Springer International Publishing. https://doi.org/10.1007/978-3-030-41579-2_18

Abraham, A., More, S., Rabensteiner, C., & Hörandner, F. (2020). *Revocable and Offline-Verifiable Self-Sovereign Identities*. *Vol. 1*, 1020–1027. https://doi.org/10.1109/TrustCom50675.2020.00136

Ahmad, S., Abdullah, S. A. J., & Arshad, R. B. (2015). Issues and challenges of transition to e-voting technology in Nigeria. *Public Policy and Administration Research*, *5*(4), 95–102.

Ahmad, S. Z., & Khalid, K. (2017). The adoption of M-government services from the user's perspectives: Empirical evidence from the United Arab Emirates. *International Journal of Information Management*, *37*(5), 367–379. https://doi.org/10.1016/j.ijinfomgt.2017.03.008

AlBar, A. M., & A., M. (2018). Exploring Saudi Citizens' Acceptance of Mobile Government Service. *International Journal of Advanced Computer Science and Applications*, *9*(11). https://doi.org/10.14569/IJACSA.2018.091156

Al-dalahmeh, M., Al-Shamaileh, O., Aloudat, A., & Obeidat, B. Y. (2018). The Viability of Mobile Services (SMS and Cell Broadcast) in Emergency Management Solutions: An Exploratory Study. *International Journal of Interactive Mobile Technologies (IJIM)*, *12*(1), 95. https://doi.org/10.3991/ijim.v12i1.7677

Alharbi, A. S., Halikias, G., Yamin, M., & Basahel, A. (2020). An overview of M-government services in Saudi Arabia. *International Journal of Information Technology*, *12*(4), 1237–1241. https://doi.org/10.1007/s41870-020-00433-9

Al-Hubaishi, H. S., Ahmad, S. Z., & Hussain, M. (2018). Assessing M-Government Application Service Quality and Customer Satisfaction. *Journal of Relationship Marketing*, *17*(3), 229–255. https://doi.org/10.1080/15332667.2018.1492323

Allen, C. (2016). The path to self-sovereign identity. *Life with Alacrity*. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Draft

Almaiah, M., Al-Khasawneh, A., Althunibat, A., & Khawatreh, S. (2020). *Mobile government adoption model based on combining GAM and UTAUT to explain factors according to adoption of mobile government services*.

Almarashdeh, I. (2020). The effect of recovery satisfaction on citizens loyalty perception: A case study of mobile government services. *International Journal of Electrical and Computer Engineering (IJECE)*, *10*(4), 4279. https://doi.org/10.11591/ijece.v10i4.pp4279-4295

Almarashdeh, I., & Alsmadi, M. K. (2017). How to make them use it? Citizens acceptance of M-government. *Applied Computing and Informatics*, *13*(2), 194–199. https://doi.org/10.1016/j.aci.2017.04.001

Alonso, A., Pozo, A., Choque, J., Bueno, G., Salvachua, J., Diez, L., Marin, J., & Alonso, P. L. C. (2019). An Identity Framework for Providing Access to FIWARE OAuth 2.0-Based Services According to the eIDAS European Regulation. *IEEE Access*, *7*, 88435–88449. https://doi.org/10.1109/ACCESS.2019.2926556

Alqaralleh, B., Al-Omari, A., & Alksasbeh, M. (2020). *An Integrated Conceptual Model for m-Government Acceptance in Developing Countries: The Case Study of Jordan*.

Alsaadi, M. R., Ahmad, S. Z., & Hussain, M. (2019). Improving the quality of mobile government services in the Gulf Cooperation Council: A quality-function-deployment approach. *Journal of Systems and Information Technology*, *21*(1), 146–164. https://doi.org/10.1108/JSIT-11-2017-0116

Andraško, J. (2017). *MUTUAL RECOGNITION OF ELECTRONIC IDENTIFICATION MEANS UNDER THE EIDAS REGULATION AND ITS APPLICATION ISSUES*. *Vol. 7*, 9–13.

Azeez, N. D., & Lakulu, M. M. (2005). EVALUATION FRAMEWORK OF M-GOVERNMENT SERVICES SUCCESS IN MALAYSIA. . . *Vol.*, *24*, 33.

Berbecaru, D., Lioy, A., & Cameroni, C. (2019). Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure. *Information*, *10*(6), 210. https://doi.org/10.3390/info10060210

Bertino, E., & Takahashi, K. (2011). *Identity management: Concepts, technologies, and systems*. Artech House.

Bharosa, N., Lips, S., & Draheim, D. (2020). Making e-Government Work: Learning from the Netherlands and Estonia. In S. Hofmann, C. Csáki, N. Edelmann, T. Lampoltshammer, U. Melin, P. Parycek, G. Schwabe, & E. Tambouris (Eds.), *Electronic Participation* (Vol. 12220, pp. 41–53). Springer International Publishing. https://doi.org/10.1007/978-3-030-58141-1_4

Blackman, M. (2006). Municipalities move to mobile government. *Government Procurement*, *14*(6), 54–55.

Draft

Boehm, O., Caumanns, J., Franke, M., & Pfaff, O. (2008). Federated Authentication and Authorization: A Case Study. *2008 12th International IEEE Enterprise Distributed Object Computing Conference*, 356–362. https://doi.org/10.1109/EDOC.2008.36

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A Hermeneutic Approach for Conducting Literature Reviews and Literature Searches. *Communications of the Association for Information Systems*, *34*. https://doi.org/10.17705/1CAIS.03412

Bradley, J., & Denniss, W. (2017). *OAuth 2.0 for Native Apps*. https://tools.ietf.org/html/rfc8252

Brands, S. A. (2000). *Rethinking public key infrastructures and digital certificates: Building in privacy*. MIT Press.

Cabarcos, P., Mendoza, F., Guerrero, R., Lopez, A., & Diaz-Sanchez, D. (2012). SuSSo: Seamless and ubiquitous single sign-on for cloud service continuity across devices. *IEEE Transactions on Consumer Electronics*, *58*(4), 1425–1433. https://doi.org/10.1109/TCE.2012.6415016

Camenisch, J., & Lysyanskaya, A. (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In B. Pfitzmann (Ed.), *Advances in Cryptology—EUROCRYPT 2001* (pp. 93–118). Springer Berlin Heidelberg.

Camilleri, M. A. (2019). The online users' perceptions toward electronic government services. *Journal of Information, Communication and Ethics in Society*, *18*(2), 221–235. https://doi.org/10.1108/JICES-09-2019-0102

Carolina, M. U. of S. (2017). *FHIR Apps for Bioresearch*. https://www.hl7.org/events/fhir/roundtable/2017/03/pdfs/D-22_Doug-Williams.pdf

Cave, J., Botterman, M., Cavalini, S., & Volpe, M. (2017). *EU-wide digital Once-Only Principle for citizens and businesses*. 273.

Chanana, L., Agrawal, R., & Punia, D. K. (2016). Service Quality Parameters for Mobile Government Services in India. *Global Business Review*, *17*(1), 136–146. https://doi.org/10.1177/0972150915610702

Chen, Z.-J., Vogel, D., & Wang, Z.-H. (2016). How to satisfy citizens? Using mobile government to reengineer fair government processes. *Decision Support Systems*, *82*, 47–57. https://doi.org/10.1016/j.dss.2015.11.005

Chiou, S.-Y., Wang, T.-J., & Chen, J.-M. (2017). Design and Implementation of a Mobile Voting System Using a Novel Oblivious and Proxy Signature. *Security and Communication Networks*, *2017*, 1–16. https://doi.org/10.1155/2017/3075210

Corici, A. A., Rode, O., Kraufmann, B., Billig, A., Caumanns, J., Deglmann, M., Walter, V., Rexin, J., & Nolte, G. (2020). *Interoperable and discrete eHealth Data Exchange between Hospital and Patient*. 168–170. https://doi.org/10.1109/ICIN48450.2020.9059335

Draft

Dai, W., Wang, Q., Wang, Z., Lin, X., Zou, D., & Jin, H. (2021). Trustzone-based secure lightweight wallet for hyperledger fabric. *Journal of Parallel and Distributed Computing*, *149*, 66–75. https://doi.org/10.1016/j.jpdc.2020.11.001

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340.

DE4A. (2020). *Digital Europe for All (DE4A)*. DE4A. https://www.de4a.eu

Decat, M., Lagaisse, B., Van Landuyt, D., Crispo, B., & Joosen, W. (2013). Federated Authorization for Software-as-a-Service Applications. In R. Meersman, H. Panetto, T. Dillon, J. Eder, Z. Bellahsene, N. Ritter, P. De Leenheer, & D. Dou (Eds.), *On the Move to Meaningful Internet Systems: OTM 2013 Conferences* (Vol. 8185, pp. 342–359). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-41030-7_25

Dhamija, R., & Dusseault, L. (2008). The Seven Flaws of Identity Management: Usability and Security Challenges. *IEEE Security & Privacy Magazine*, *6*(2), 24–29. https://doi.org/10.1109/MSP.2008.49

DIACC. (2021). *Decentralized Identity and DIACC PCTF Authentication*. https://diacc.ca/2021/02/22/decentralized-identity-and-diacc-pctf-authentication/

DIF. (2020). *DIF - Steering Committee*. https://identity.foundation/governance/about

EBSI. (2021). *European Blockchain Services Infrastructure*. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

EHDSI. (2020). *Semantic Services Specification—EHealth DSI Operations—CEF Digital*. https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Semantic+Services+Specification

Eid, R., Selim, H., & El-Kassrawy, Y. (2020). Understanding citizen intention to use m-government services: An empirical study in the UAE. *Transforming Government: People, Process and Policy*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/TG-10-2019-0100

El-Kiki, T., & Lawrence, E. (2006). Mobile user satisfaction & usage anlysis model of MGovernment services. *Verified OK*.

ESSIF. (2021). *European Self-Sovereign Identity Framework*. CEF Digital. https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/pages/viewpage.action?pageId=262505360

ETSI. (2020a). *ETSI Specialist Task Force 588*. https://portal.etsi.org/STF/STFs/STF-HomePages/STF588

ETSI. (2020b). *ETSI TR 119 461* [Technical specification]. https://docbox.etsi.org/esi/Open/Latest_Drafts/Draft%20ETSI-TS-119-461-v0.0.5.pdf

ETSI. (2021). *ETSI TR 119 460* [Technical report]. https://www.etsi.org/deliver/etsi_tr/119400_119499/119460/01.01.01_60/tr_119460v010101p.pdf

Draft

EUCARIS. (2021). *Home*. https://www.eucaris.net/

Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Pub. L. No. 2014/910/EU (2014). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

European Commission. (2014, July 7). *Cross-border health project epSOS: What has it achieved?* [Text]. Shaping Europe's Digital Future - European Commission. https://ec.europa.eu/digital-single-market/en/news/cross-border-health-project-epsos-what-has-it-achieved

European Commission. (2015). *A Digital Single Market Strategy for Europe*. 20.

European Commission. (2016). *The use of CEF eID in the CEF eHealth DSI Final Report*.

European Commission. (2017). *Tallinn Declaration on eGovernment* (p. 14).

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, Pub. L. No. 2018/1724/EU (2018). http://data.europa.eu/eli/reg/2018/1724/oj

European Commission. (2019). *EIDAS Interoperability Architecture* (v. 1.2). https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf

European Commission. (2020). *Berlin Declaration on Digital Society and Value-based Digital Government* (p. 16).

European Commission. (2021). *Electronic Exchange of Social Security Information (EESSI)*.

Ferdous, Md. S., & Poet, R. (2012). A comparative analysis of Identity Management Systems. *2012 International Conference on High Performance Computing & Simulation (HPCS)*, 454–461. https://doi.org/10.1109/HPCSim.2012.6266958

FIDO Alliance. (2017, April 11). *Universal 2nd Factor (U2F) Overview*. https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.pdf

FIDO Alliance. (2019, January 30). *Client to Authenticator Protocol (CTAP)*. https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html

FIDO Alliance. (2020, October 20). *FIDO UAF Architectural Overview*. https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-overview-v1.2-ps-20201020.html

Fishbein, M., & Ajzen, I. (1977). *Belief, attitude, intention, and behavior: An introduction to theory and research*.

Draft

Fraunhofer FOKUS. (2021). *Telehealth | CTS2-LE*. https://www.innovationszentrum-telehealth.de/go/cts2

Glood, S. H., Osman, W. R. S., & Nadzir, M. M. (2005). THE EFFECT OF CIVIL CONFLICTS AND NET BENEFITS ON M-GOVERNMENT SUCCESS OF DEVELOPING COUNTRIES: A CASE STUDY OF IRAQ. . . *Vol.*, 12.

Goodner, M., & Nadalin, A. (2009). *Web Services Federation Language (WS-Federation)* (Version 1.2). OASIS. http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines: Revision 3* (NIST SP 800-63-3; p. NIST SP 800-63-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

Hardjono, T., Maler, E., Machulak, M., & Catalano, D. (2015, December 28). *OAuth 2.0 Resource Set Registration*. https://docs.kantarainitiative.org/uma/rec-oauth-resource-reg-v1_0_1.html

Hardjono, Thomas. (2012). *User-Managed Access (UMA) Profile of OAuth 2.0*.

Helger, P. (2021). *Setup Peppol AP*. https://peppol.helger.com/public/menuitem-docs-setup-ap

Hilgers, D., & Schmidthuber, L. (2018). Open Government: Exploring Patterns of Mobile Interaction Between Citizens and Local Government. In H. Albach, H. Meffert, A. Pinkwart, R. Reichwald, & Ł. Świątczak (Eds.), *European Cities in Dynamic Competition* (pp. 57–72). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-56419-6_4

HL7 International. (2020, May 19). *International Patient Summary HL7 FHIR Profile definition*. http://hl7.org/fhir/uv/ips/

Hou, J. (Jove), Arpan, L., Wu, Y., Feiock, R., Ozguven, E., & Arghandeh, R. (2020). The Road toward Smart Cities: A Study of Citizens' Acceptance of Mobile Applications for City Services. *Energies*, *13*(10), 2496. https://doi.org/10.3390/en13102496

IETF. (2007). *Open Authorization 1.0 (OAuth 1.0)*. https://oauth.net/1/

IETF. (2012). *Open Authorization 2.0 (OAuth 2.0)*. https://oauth.net/2/

Iqbal, S., Irfan, M., Ahsan, K., Hussain, M. A., Awais, M., Shiraz, M., Hamdi, M., & Alghamdi, A. (2020). A Novel Mobile Wallet Model for Elderly Using Fingerprint as Authentication Factor. *IEEE Access*, *8*, 177405–177423. https://doi.org/10.1109/ACCESS.2020.3025429

Ishengoma, F., Mselle, L., & Mongi, H. (2019). Critical success factors for m-Government adoption in Tanzania: A conceptual framework. *The Electronic Journal of Information Systems in Developing Countries*, *85*(1), e12064. https://doi.org/10.1002/isd2.12064

ISO. (2012). *ISO/IEC 29191:2012*. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/52/45270.html

Draft

ISO. (2013). *ISO/IEC 29115:2013*. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/51/45138.html

ISO. (2018). *ISO/IEC TS 29003:2018*. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/22/62290.html

ISO. (2019). *ISO/IEC 24760-1:2019*. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/75/77582.html

ISO. (2020). *ISO/IEC FDIS 18013-5:2020*. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/90/69084.html

Iyamu, T. (2020). Creating a technical architecture framework for m-voting application. *African Journal of Science, Technology, Innovation and Development*, 1–8. https://doi.org/10.1080/20421338.2020.1812977

Joinup. (2021). *About CEF eDelivery*. https://joinup.ec.europa.eu/collection/connecting-europe-facility-cef/solution/cef-edelivery/about

Jøsang, A., Zomai, M. A., & Suriadi, S. (2007). Usability and Privacy in Identity Management Architectures. *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers - Volume 68*, 143–152.

Kaasinen, E. (2005). *User acceptance of mobile services: Value, ease of use, trust and ease of adoption*. Citeseer.

Kalvet, T., Toots, M., Krimmer, R., & Cepilovs, A. (2018). *Position Paper on Definition of OOP and Situation in Europe (updated version)*. 21.

Krawczyk, H. (2003). SIGMA: The 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols. In D. Boneh (Ed.), *Advances in Cryptology—CRYPTO 2003* (pp. 400–425). Springer Berlin Heidelberg.

Krimmer, R., Kalvet, T., & Toots, M. (2018). Contributing to a digital single market for Europe Barriers and Drivers of an EU-wide Once-Only Principle. *Dg.o '18: Dg.o 2018: Proceedings Ofthe 19th Annual International Conference on Digital Government Research, May 30-June 1, 2018,* 1–8. https://doi.org/10.1145/3209281.3209344

Kumar, A., & Srivastava, A. K. (2011). Designing and developing secure protocol for mobile voting. *International Journal of Applied Engineering Reesearch*.

Kumar, M., & Sinha, O. P. (2007). M-government–mobile technology for e-government. *International Conference on E-Government, India*, 294–301.

Lenz, T. (2016). *ENHANCING CROSS-BORDER EID FEDERATIONS BY USING A MODULAR AND FLEXIBLE ATTRIBUTE MAPPING SERVICE TO MEET NATIONAL LEGAL AND TECHNICAL REQUIREMENTS. Vol. 13*(No. 2), 52.

Draft

Lenz, T., & Alber, L. (2017). Towards Cross-Domain eID by Using Agile Mobile Authentication. *2017 IEEE Trustcom/BigDataSE/ICESS*, 570–577. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.286

Lenz, T., & Krnjic, V. (2019). Torwards Flexible Multi-factor Combination for Authentication Based on Smart-Devices. In M. J. Escalona, F. Domínguez Mayo, T. A. Majchrzak, & V. Monfort (Eds.), *Web Information Systems and Technologies* (Vol. 372, pp. 221–243). Springer International Publishing. https://doi.org/10.1007/978-3-030-35330-8_11

Lenz, T., & Krnjic, V. (2018). Towards Domain-Specific and Privacy-Preserving Qualified eID in a User-Centric Identity Model. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1157–1163. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00160

Lenz, T., & Zwattendorfer, B. (2016a). Enhancing the Modularity and Flexibility of Identity Management Architectures for National and Cross-Border eID Applications. In V. Monfort, K.-H. Krempels, T. A. Majchrzak, & Ž. Turk (Eds.), *Web Information Systems and Technologies* (Vol. 246, pp. 123–143). Springer International Publishing. https://doi.org/10.1007/978-3-319-30996-5_7

Lenz, T., & Zwattendorfer, B. (2016b). Towards Cross-Border Authorization in European eID Federations. *2016 IEEE Trustcom/BigDataSE/ISPA*, 426–434. https://doi.org/10.1109/TrustCom.2016.0093

Leroux, M., H. ,. Metke-Jimenez, A. &. Lawley. (2017). Towards achieving semantic interoperability of clinical study data with FHIR. *Journal of Biomedical Semantics*. https://jbiomedsem.biomedcentral.com/articles/10.1186/s13326-017-0148-7

Mamrot, S., & Rzyszczak. (2020). *Implementation of the 'once-only' Principle in Europe – national approach*.

Mandari, H. E., Chong, Y.-L., & Wye, C.-K. (2017). The influence of government support and awareness on rural farmers' intention to adopt mobile government services in Tanzania. *Journal of Systems and Information Technology*, *19*(1/2), 42–64. https://doi.org/10.1108/JSIT-01-2017-0005

Mishra, S., & Singh, M. (2019). A conceptual framework for effective m-governance. *Journal of Engineering Science and Technology*, *14*(6), 3514–3535.

MobileConnect. (2021). *MobileConnect*. MobileConnect. https://mobileconnect.io/

Mocanu, S., Chiriac, A. M., Popa, C., Dobrescu, R., & Saru, D. (2019). Identification and Trust Techniques Compatible with eIDAS Regulation. In J. Li, Z. Liu, & H. Peng (Eds.), *Security and Privacy in New Computing Environments* (pp. 656–665). Springer International Publishing.

Draft

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & for the PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ*, *339*(jul21 1), b2535–b2535. https://doi.org/10.1136/bmj.b2535

Morgner, F., Bastian, P., & Fischlin, M. (2016). Attribute-Based Access Control Architectures with the eIDAS Protocols. In L. Chen, D. McGrew, & C. Mitchell (Eds.), *Security Standardisation Research* (Vol. 10074, pp. 205–226). Springer International Publishing. https://doi.org/10.1007/978-3-319-49100-4_9

Mossey, S., Bromberg, D., & Manoharan, A. P. (2019). Harnessing the power of mobile technology to bridge the digital divide: A look at U.S. cities' mobile government capability. *Journal of Information Technology & Politics*, *16*(1), 52–65. https://doi.org/10.1080/19331681.2018.1552224

Mozilla. (2013). *BrowserID*. https://github.com/mozilla/id-specs

Mudda, M., & Bhargava Choubey, S. (2018). Application of System Engineering in Election Voting System. *International Journal of Engineering & Technology*, *7*(2.16), 102. https://doi.org/10.14419/ijet.v7i2.16.11503

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Ndou, V. (2004). E–Government for developing countries: Opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries*, *18*(1), 1–24.

NIST. (2019). *Mobile Application Single Sign-On* (NIST SPECIAL PUBLICATION 1800-13). https://www.nccoe.nist.gov/publication/1800-13/index.html

Ntaliani, M., Costopoulou, C., & Karetsos, S. (2008). Mobile government: A challenge for agriculture. *Government Information Quarterly*, *25*(4), 699–716.

OASIS. (2021). *Service Metadata Publishing (SMP) Version 2.0*. https://www.oasis-open.org/2021/02/17/service-metadata-publishing-smp-version-2-0-oasis-standard-published/

OECD. (2007). *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*. http://www.oecd.org/sti/ieconomy/38921342.pdf

OECD. (2011). *Digital identity management for natural persons: Enabling innovation and trust in the Internet economy*. http://www.oecd.org/sti/ieconomy/49338380.pdf

OECD, & International Telecommunication Union. (2011). *M-Government: Mobile Technologies for Responsive Governments and Connected Societies*. OECD. https://doi.org/10.1787/9789264118706-en

Onashoga, A., Ogunjobi, A., Ibharalu, T., & Lawal, O. (2016). A secure framework for SMS-based service delivery in m-government using a multicast encryption scheme. *African Journal of Science,*

Draft

Technology, Innovation and Development, *8*(3), 247–255. https://doi.org/10.1080/20421338.2016.1156837

OpenID, F. (2021). *OpenID Specifications*. https://openid.net/developers/specs/

OpenPEPPOL. (2021). *PEPPOL eDelivery Network—An Overview—Peppol*. https://peppol.eu/what-is-peppol/peppol-transport-infrastructure/

Pöhn, D., & Hommel, W. (2020). IMC: A Classification of Identity Management Approaches. In I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, & A. Sasse (Eds.), *Computer Security* (Vol. 12580, pp. 3–20). Springer International Publishing. https://doi.org/10.1007/978-3-030-66504-3_1

Ragouzis, N., Hughes, J., Philpott, R., Maler, E., Madsen, P., & Scavo, T. (2008). *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. OASIS. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

Rashid, N. (2020). *Deploying the Once-Only Policy*. 61.

Reddick, C. G., & Zheng, Y. (2017). Determinants of citizens' mobile apps future use in Chinese local governments: An analysis of survey data. *Transforming Government: People, Process and Policy*, *11*(2), 213–235. https://doi.org/10.1108/TG-11-2016-0078

Rocha, J. (2020). Spanish and portuguese eIDAS node evolution for electronic identification of European citizens. *Proceedings of the 10th Euro-American Conference on Telematics and Information Systems*, 1–5. https://doi.org/10.1145/3401895.3402094

Rodrigues Frade, J. (2016). *Electronic Registered Delivery Service (ERDS) and the eIDAS Regulation*. https://ec.europa.eu/cefdigital/wiki/download/attachments/32052812/CEF%20eDelivery%20Live%20Webinar%20-%20ERDS%20and%20the%20eIDAS%20Regulation.pdf?version=1&modificationDate=1473689858106&api=v2

Roelofs, F. (2019). *Analysis and comparison of identification and authentication systems under the eIDAS regulation* [Master thesis, Radboud University]. https://www.ru.nl/publish/pages/769526/z02_masterthesis_floris_roelofs_final.pdf

Rogers, E. M. (1995). Diffusion of Innovations: Modifications of a Model for Telecommunications. In M.-W. Stoetzer & A. Mahler (Eds.), *Die Diffusion von Innovationen in der Telekommunikation* (pp. 25–38). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-79868-9_2

Ryu, S., Hong, P., & Lim, T. (2020). Changes and directions of ict services in Korea government. *ICIC Express Letters, Part B: Applications*, *11*, 683–689.

Saadi, M. R., Ahmad, S. Z., & Hussain, M. (2017). Prioritization of citizens' preferences for using mobile government services: The analytic hierarchy process (AHP) approach. *Transforming*

Draft

Government: People, Process and Policy, *11*(3), 476–503. https://doi.org/10.1108/TG-04-2017-0020

Saeb Al-Sherideh, A., Ismail, R., Abdul Wahid, F., Fabil, N., & Ismail, W. (2018). Mobile Government Applications Based on Security and Privacy: A Literature Review. *International Journal of Engineering & Technology*, *7*(4.1), 51. https://doi.org/10.14419/ijet.v7i4.1.19492

Sareen, M., Punia, D. K., & Chanana, L. (2013). Exploring factors affecting use of mobile government services in India. *Problems and Perspectives in Management*, *11, Iss. 4*, 86–93.

Satybaldy, A., Nowostawski, M., & Ellingsen, J. (2020). Self-Sovereign Identity Systems: Evaluation Framework. In M. Friedewald, M. Önen, E. Lievens, S. Krenn, & S. Fricker (Eds.), *Privacy and Identity Management. Data for Better Living: AI and Privacy* (Vol. 576, pp. 447–461). Springer International Publishing. https://doi.org/10.1007/978-3-030-42504-3_28

Saxena, S. (2018). Role of "perceived risks" in adopting mobile government (m-government) services in India. *Foresight*, *20*(2), 190–205. https://doi.org/10.1108/FS-08-2017-0040

Shahzad, F., Xiu, G., Shafique Khan, M. A., & Shahbaz, M. (2020). Predicting the adoption of a mobile government security response system from the user's perspective: An application of the artificial neural network approach. *Technology in Society*, *62*, 101278. https://doi.org/10.1016/j.techsoc.2020.101278

Shareef, M. A., Dwivedi, Y. K., Laumer, S., & Archer, N. (2016). Citizens' Adoption Behavior of Mobile Government (mGov): A Cross-Cultural Study. *Information Systems Management*, *33*(3), 268–283. https://doi.org/10.1080/10580530.2016.1188573

Shareef, M. A., Kumar, V., Kumar, U., & Dwivedi, Y. K. (2011). e-Government Adoption Model (GAM): Differing service maturity levels. *Government Information Quarterly*, *28*(1), 17–35. https://doi.org/10.1016/j.giq.2010.05.006

Soltani, R., Nguyen, U. T., & An, A. (2019). Practical Key Recovery Model for Self-Sovereign Identity Based Digital Wallets. *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 320–325. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066

Sovrin Foundation. (2021). *Sovrin*. Sovrin. https://sovrin.org/

Styrin, E., & Kostyrko, A. (2016). Implementing Smart Services in Moscow: The Integrated Mobile Platform. In J. R. Gil-Garcia, T. A. Pardo, & T. Nam (Eds.), *Smarter as the New Urban Agenda* (Vol. 11, pp. 225–241). Springer International Publishing. https://doi.org/10.1007/978-3-319-17620-8_12

Sultana, M. R., Ahlan, A. R., & Habibullah, M. D. (2016). A Comprehensive Adoption Model of M-Government Services Among Citizens In Developing Countries. *Journal of Theoretical & Applied Information Technology*, *90*(1).

Draft

Talukder, S., Chiong, R., Dhakal, S., Sorwar, G., & Bao, Y. (2019). A two-stage structural equation modeling-neural network approach for understanding and predicting the determinants of m-government service adoption. *Journal of Systems and Information Technology*, *21*(4), 419–438. https://doi.org/10.1108/JSIT-10-2017-0096

The Linux Foundation. (2020a). Hyperledger Aries. *Hyperledger*. https://www.hyperledger.org/use/aries

The Linux Foundation. (2020b). *Hyperledger Indy*. https://www.hyperledger.org/use/hyperledger-indy

TOOP, P. (2018). *Information System Architecture*. http://wiki.ds.unipi.gr/display/TOOPRA/IS+Architecture

TOOP, P. (2019). *Network and Communication*. http://wiki.ds.unipi.gr/display/TOOPRA24INT/Network+Overview

TOOP, P. (2020a). *Core Vocabularies and Application Profiles*. http://wiki.ds.unipi.gr/display/TOOPSA21OOP/.Core+Vocabularies+and+Application+Profiles+v2.0.1

TOOP, P. (2020b). *Criterion & Evidence Type Rule Base*. http://wiki.ds.unipi.gr/display/TOOPSA210CEF/Criterion+And+Evidence+Type+Rule+Base

TOOP, P. (2020c). *New SMP Deployment and Configuration Guide*. http://wiki.ds.unipi.gr/display/CCTF/New+SMP+Deployment+and+Configuration+Guide

TOOP, P. (2020d). *Technical Implementation*. http://wiki.ds.unipi.gr/display/TOOPSA21OOP/Technical+Implementation

TOOP, P. (2020e). *Use of Semantics in Services and Components*. http://wiki.ds.unipi.gr/display/TOOPSA21OOP/.Use+of+Semantics+in+Services+and+Components+v2.0.1

TOOP, P. (2021). *Greek PEPPOL Directory*. http://directory.acc.exchange.toop.eu/public/locale-en_US/menuitem-docs-introduction

Trimi, S., & Sheng, H. (2008). Emerging trends in M-government. *Communications of the ACM*, *51*(5), 53–58.

Tsakalakisz, N., Stalla-Bourdillon, S., & O'Hara, K. (2017). Identity Assurance in the UK: Technical implementation and legal implications under eIDAS. *Journal of Web Science*, *3*(1), 32–46. https://doi.org/10.1561/106.00000010

Tseng, P. T. Y., Yen, D. C., Hung, Y.-C., & Wang, N. C. F. (2008). To explore managerial issues and their implications on e-Government deployment in the public sector: Lessons from Taiwan's Bureau of Foreign Trade. *Government Information Quarterly*, *25*(4), 734–756. https://doi.org/10.1016/j.giq.2007.06.003

Draft

United Nations. (2020). *A/CN.9/WG.IV/WP.162*. 18.

UPort. (2021). https://developer.uport.me/

Van, H. T., Kim, M. B., Sa, J.-H., Kim, J.-B., & Gim, G. (2016). The Factors Affecting User Behavior on Mobile Voting in Vietnam. *International Journal of Multimedia and Ubiquitous Engineering*, *11*(6), 311–318. https://doi.org/10.14257/ijmue.2016.11.6.27

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425–478.

W3C. (2019, November 19). *Verifiable Credentials Data Model 1.0*. https://www.w3.org/TR/vc-data-model/

W3C. (2021a, February 25). *Web Authentication: An API for accessing Public Key Credentials—Level 2*. https://www.w3.org/TR/webauthn/

W3C. (2021b, March 18). *Decentralized Identifiers (DIDs) v1.0*. https://www.w3.org/TR/did-core/#architecture-overview

Wang, C. (2014). Antecedents and consequences of perceived value in Mobile Government continuance use: An empirical research in China. *Computers in Human Behavior*, *34*, 140–147.

Wang, C., Teo, T. S. H., & Liu, L. (2020). Perceived value and continuance intention in mobile government service in China. *Telematics and Informatics*, *48*, 101348. https://doi.org/10.1016/j.tele.2020.101348

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Wimmer, M. A., Neuroni, A. C., & Frecè, J. T. (2020). Approaches to Good Data Governance in Support of Public Sector Transformation Through Once-Only. In G. Viale Pereira, M. Janssen, H. Lee, I. Lindgren, M. P. Rodríguez Bolívar, H. J. Scholl, & A. Zuiderwijk (Eds.), *Electronic Government* (Vol. 12219, pp. 210–222). Springer International Publishing. https://doi.org/10.1007/978-3-030-57599-1_16

Windley, P., & Reed, D. (2018). *Sovrin: A protocol and token for self-sovereign identity and decentralized trust*. The Sovrin Foundation. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

Wirtz, B. W., Birkmeyer, S., & Langer, P. F. (2019). Citizens and mobile government: An empirical analysis of the antecedents and consequences of mobile government usage. *International Review of Administrative Sciences*, 0020852319862349.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, *22*(1), 45–55. https://doi.org/10.1057/ejis.2011.51

Draft

Yaagesh Prasad, P., & Malathi, S. (2020). M-Voting with Government Authentication System. In D. J. Hemanth, V. D. A. Kumar, S. Malathi, O. Castillo, & B. Patrut (Eds.), *Emerging Trends in Computing and Expert Technology* (Vol. 35, pp. 1244–1259). Springer International Publishing. https://doi.org/10.1007/978-3-030-32150-5_126

Draft

Annex I

Table 4: Key factor Quality and identified components

Key Factor	Components	References
Quality	Service Quality	(Al-Hubaishi et al., 2018, p.); (Chanana et al., 2016); (Alqaralleh et al., 2020); (Azeez & Lakulu, 2005); (AlBar & A., 2018); (Almarashdeh, 2020); (Alsaadi et al., 2019); (Glood et al., 2005); (Saxena, 2018); (Wirtz et al., 2019)
	Outcome Quality	(Al-Hubaishi et al., 2018); (Alsaadi et al., 2019)
	Information Quality	(Shahzad et al., 2020); (Almaiah et al., 2020); (Azeez & Lakulu, 2005); (Al-Hubaishi et al., 2018); (AlBar & A., 2018); (Glood et al., 2005)
	Service Recovery	(Almarashdeh, 2020)
	Reliability	(Alharbi et al., 2020)
	Service Ubiquity	(Alharbi et al., 2020); (Camilleri, 2019)
	Information Accuracy	(Z.-J. Chen et al., 2016)

Table 5: Key factor Provision and identified components

Key Factor	Components	References
Provision	Lack of legal framework and structure	(Onashoga et al., 2016); (Saxena, 2018)
	Policy Framework	(Ryu et al., 2020)
	Distributive and Interactional Justice	(Almarashdeh, 2020)
	Government Support	(Mandari et al., 2017)

Table 6: Key factor Perceived Value and identified components

Key Factor	Components	References
Perceived Value	Citizens expectations	(Alsaadi et al., 2019)
	Perceived Value	(Almarashdeh, 2020); (Wang et al., 2020)
	Increased channels for interaction	(Almarashdeh, 2020); (Alsaadi et al., 2019)
	Enhancing civic engagement among citizens	(AlBar & A., 2018)
	Cost	(Ishengoma et al., 2019); (AlBar & A., 2018); (Almarashdeh, 2020); (Glood et al., 2005); (Hou et al., 2020);

Draft

Key Factor	Components	References
		(Mudda & Bhargava Choubey, 2018); (Saxena, 2018); (Wang et al., 2020); (Almarashdeh & Alsmadi, 2017)
	Voice opportunity	(Z.-J. Chen et al., 2016)
	Belief they will benefit by using mGov	(Alharbi et al., 2020); (Glood et al., 2005)
	Demand for government applications	(Reddick & Zheng, 2017)
	Citizen participation	(Alsaadi et al., 2019)

Table 7: Key factor Demographics and identified components

Key Factor	Components	References
Demographics	Gender	(S. Z. Ahmad & Khalid, 2017); (Saxena, 2018)
	Age	(S. Z. Ahmad & Khalid, 2017); (Saxena, 2018)
	Household Income	(S. Z. Ahmad & Khalid, 2017)
	Poverty	(Mossey et al., 2019)
	Limited human skills development	(Onashoga et al., 2016); (Almarashdeh, 2020)
	Education	(Mossey et al., 2019); (Saxena, 2018)
	Minorities	(Mossey et al., 2019)
	Digital divide	(Almarashdeh, 2020); (Camilleri, 2019); (Chiou et al., 2017); (Glood et al., 2005)

Table 8: Key factor Trust and identified components

Key Factor	Components	References
Trust	Trust in technology	(Almarashdeh & Alsmadi, 2017); (Saeb Al-Sherideh et al., 2018); (Eid et al., 2020); (Mishra & Singh, 2019); (Onashoga et al., 2016); (Shahzad et al., 2020); (Alqaralleh et al., 2020); (Almarashdeh, 2020)
	Trust	(S. Z. Ahmad & Khalid, 2017); (Almaiah et al., 2020); (Alqaralleh et al., 2020); (Azeez & Lakulu, 2005); (AlBar & A., 2018); (Almarashdeh, 2020); (Iyamu,

Draft

Key Factor	Components	References
		2020); (A. Kumar & Srivastava, 2011); (Saxena, 2018)
	Trust in government	(Alqaralleh et al., 2020); (Almarashdeh, 2020); (Hou et al., 2020)
	Transparency	(Mishra & Singh, 2019); (Shahzad et al., 2020); (Z.-J. Chen et al., 2016); (Alharbi et al., 2020); (Wang et al., 2020)
	Perceived risk	(Almarashdeh, 2020); (Saxena, 2018)
	Perceived reliability	(Shareef et al., 2016); (Z.-J. Chen et al., 2016)
	Procedural fairness	(Z.-J. Chen et al., 2016)

Table 9: Key factor User Experience and identified components

Key Factor	Components	References
User experience	Personalization	(Wang et al., 2020)
	User centricity	(Wang et al., 2020)
	Information overload	(Saxena, 2018)
	Simplicity	(Mudda & Bhargava Choubey, 2018)
	Responsiveness	(Alharbi et al., 2020)
	Citizen Satisfaction	(Alqaralleh et al., 2020); (Azeez & Lakulu, 2005); (Reddick & Zheng, 2017); (AlBar & A., 2018); (Van et al., 2016)
	Perceived effectiveness	(Azeez & Lakulu, 2005); (Wang et al., 2020)
	Performance expectancy	(Almaiah et al., 2020); (Hou et al., 2020); (Talukder et al., 2019)
	Effort expectancy	(AlBar & A., 2018); (Almaiah et al., 2020); (Hou et al., 2020); (Talukder et al., 2019)
	Self-efficacy	(Almaiah et al., 2020); (Almarashdeh, 2020); (Saxena, 2018)
	Convenience	(Shahzad et al., 2020); (Reddick & Zheng, 2017); (Glood et al., 2005); (Van et al., 2016)
	Perceived Ease of Use (PEOU)	(Eid et al., 2020); (Hilgers & Schmidthuber, 2018); (Mishra & Singh, 2019); (Alqaralleh et al., 2020); (Z.-J. Chen et al., 2016); (Ishengoma et al., 2019); (Mandari et al., 2017); (Shareef et al., 2016); (AlBar & A., 2018); (Alharbi

Draft

Key Factor	Components	References
		et al., 2020); (Glood et al., 2005); (Ryu et al., 2020)
	Perceived Usefulness	(AlBar & A., 2018); (Almarashdeh & Alsmadi, 2017); (Alqaralleh et al., 2020); (Saeb Al-Sherideh et al., 2018); (Eid et al., 2020); (Mishra & Singh, 2019); (Shareef et al., 2016)
	Trialability	(Mandari et al., 2017)
	Perceived Compatibility	(Mishra & Singh, 2019); (Almaiah et al., 2020); (Alqaralleh et al., 2020); (Mandari et al., 2017); (AlBar & A., 2018)
	User Acceptance	(Almarashdeh & Alsmadi, 2017)

Table 10: Key factor Mobile Strengths and identified components

Key Factor	Components	References
Mobile Strengths	Mobility	(Mishra & Singh, 2019); (Saadi et al., 2017); (AlBar & A., 2018); (Alsaadi et al., 2019); (Talukder et al., 2019); (Wang et al., 2020)
	Flexibility	(Mishra & Singh, 2019)
	Immediacy	(Saadi et al., 2017); (Shahzad et al., 2020); (Alharbi et al., 2020); (Alsaadi et al., 2019); (Glood et al., 2005)
	Real time information	(Mishra & Singh, 2019); (Saadi et al., 2017); (Alsaadi et al., 2019); (Glood et al., 2005); (Hou et al., 2020); (Ryu et al., 2020); (Saxena, 2018)
	Portability	(Z.-J. Chen et al., 2016); (Alsaadi et al., 2019); (Saxena, 2018)
	Location (any)	(Iyamu, 2020); (Saxena, 2018); (Z.-J. Chen et al., 2016)
	Speed	(Ryu et al., 2020); (Saxena, 2018); (Yaagesh Prasad & Malathi, 2020)
	Convenience	(Shahzad et al., 2020); (Reddick & Zheng, 2017); (Glood et al., 2005); (Van et al., 2016)
	Access	(Ishengoma et al., 2019); (Reddick & Zheng, 2017); (Alharbi et al., 2020); (Alsaadi et al., 2019); (Glood et al., 2005); (Saxena,

Draft

Key Factor	Components	References
		2018); (Wang et al., 2020); (Styrin & Kostyrko, 2016)
	Active control	(Z.-J. Chen et al., 2016)
	Multimedia services	(Z.-J. Chen et al., 2016)
	Reachability	(A. Kumar & Srivastava, 2011); (Saxena, 2018); (Wang et al., 2020)
	Limited computational capacity of mobile devices	(Iyamu, 2020); (Saxena, 2018)
	Emergency management	(Glood et al., 2005); (Saxena, 2018)
	Tangible services	(Alsaadi et al., 2019)
	Service ubiquity	(Alharbi et al., 2020); (Camilleri, 2019)
	Timeliness	(Z.-J. Chen et al., 2016); (Alsaadi et al., 2019); (Yaagesh Prasad & Malathi, 2020); (A. Kumar & Srivastava, 2011); (AlBar & A., 2018); (Almarashdeh, 2020); (Glood et al., 2005)

Table 11: Key factor Infrastructure and identified components

Key Factor	Components	References
Infrastructure	Interoperability	(Saxena, 2018)
	Smartphone penetration	(Ryu et al., 2020); (Saxena, 2018)
	Infrastructure	(Ishengoma et al., 2019); (AlBar & A., 2018); (Camilleri, 2019); (Hou et al., 2020); (Iyamu, 2020); (Ryu et al., 2020); (Saxena, 2018); (Saeb Al-Sherideh et al., 2018); (Onashoga et al., 2016)
	Facilitating conditions	(Almaiah et al., 2020)
	Availability of resources	(Almaiah et al., 2020)

Table 12: Key factor Image and identified components

Key Factor	Components	References
Image	Relative advantage	(Mandari et al., 2017)
	Image	(Mandari et al., 2017)
	Visibility	(Mandari et al., 2017); (Alharbi et al., 2020)
	Result demonstrability	(Mandari et al., 2017)

Draft

Key Factor	Components	References
	Social Influence	(Almarashdeh & Alsmadi, 2017); (S. Z. Ahmad & Khalid, 2017); (Almarashdeh, 2020); (Hou et al., 2020)

Table 13: Key factor Attitude and identified components

Key Factor	Components	References
Attitude	Attitude	(Saxena, 2018)
	Behavioral Intention	(Saxena, 2018); (AlBar & A., 2018)
	Personal Initiative/ Characteristic	(Ishengoma et al., 2019); (Reddick & Zheng, 2017)

Table 14: Key factor Security and identified components

Key Factor	Components	References
Security	Security	(Saeb Al-Sherideh et al., 2018); (Eid et al., 2020); (Mishra & Singh, 2019); (Onashoga et al., 2016); (Saadi et al., 2017); (Almaiah et al., 2020); (Ishengoma et al., 2019); (Shareef et al., 2016); (AlBar & A., 2018); (Camilleri, 2019); (Chiou et al., 2017); (Ryu et al., 2020); (Saxena, 2018); (Yaagesh Prasad & Malathi, 2020)
	Privacy	(Saeb Al-Sherideh et al., 2018); (Onashoga et al., 2016); (Saadi et al., 2017); (Camilleri, 2019); (Iyamu, 2020); (Saxena, 2018)
	Confidentiality	(Iyamu, 2020)

Table 15: Key factor Awareness and identified components

Key Factor	Components	References
Awareness	Weak understanding of mobile government	(Saeb Al-Sherideh et al., 2018)
	Awareness or lack of awareness	(Shahzad et al., 2020); (Al-dalahmeh et al., 2018); (Almaiah et al., 2020); (Mandari et al., 2017); (AlBar & A., 2018); (Saxena, 2018)

Draft