Barriers for developing and launching digital identity wallets

Lukkien, Bert; De Reuver, Mark; Bharosa, Nitesh

DOI
10.1145/3598469.3598501

Publication date
2023

Document Version
Final published version

Published in
Proceedings of the 24th Annual International Conference on Digital Government Research - Together in the Unstable World

Barriers for developing and launching digital identity wallets

Bert Lukkien
Delft University of Technology
j.a.lukkien@tudelft.nl

Mark de Reuver
Delft University of Technology
g.a.dereuver@tudelft.nl

Nitesh Bharosa
Delft University of Technology
bharosa@tudelft.nl

ABSTRACT

Across the European continent, governments and GovTech companies are rushing to launch digital identity wallets for citizens. These wallets should allow citizens to obtain a higher level of control over their personal data. While there are some regulations and policy directions, actors are struggling with the design, launch, and governance of these digital wallets. Those looking for help will find little guidance in academic literature. The objective of this paper is to provide insights in barriers for launching digital identity wallets by a public-private ecosystem. Drawing on the case study approach, we study the available regulations and policy directions, and collect insights from workshops with policy makers and aspiring wallet providers. The main findings indicate that barriers such as the lack of boundary resources (e.g. shared data specifications and exchange standards) and the absence of a collaborative, public-private governance impede the launch of digital identity wallets. Policy makers looking to speed up the launch of digital wallets must focus on removing these barriers, starting with the development and governance of boundary resources by the public-private ecosystem.

KEYWORDS

Digital identity wallet, personal data management, public-private collaboration, barriers

ACM Reference Format:
Bert Lukkien, Mark de Reuver, and Nitesh Bharosa. 2023. Barriers for developing and launching digital identity wallets. In *24th Annual International Conference on Digital Government Research - Together in the unstable world: Digital government and solidarity (DGO 2023), July 11–14, 2023, Gdańsk, Poland*. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3598469.3598501

1 INTRODUCTION

The need to be able to share data between organizations and individuals is growing, but at the same time, the responsible handling of data is problematic. In the wake of several global data scandals (e.g. Cambridge Analytica) that have exposed the misuse of personal data, public and private parties are rushing to provide solutions for personal data management. Examples include SOLID and MyData, as well the ongoing development of privacy preserving and privacy enhancing technologies [1],[2]. High-level policy objectives include information self-determination, equal opportunities, transparency, data protection, privacy and security on the one hand, but also increasing efficiency and reducing the administrative burden for citizens and service providers play a role [3].

The first regulatory initiative in the European Union (EU) to foster responsible handling of data is the adoption of the General Data Protection Regulation (GDPR)[1]. Even though GDPR provides guidelines for collecting and processing personal data, thereby promoting the level of control by the individual, it does not provide the necessary technical tools for doing so. When it comes to tooling, another EU Regulation is setting the stage for parties to develop 'wallets'. This is the Electronic Identification and trust services for electronic transactions in the internal market (eIDAS)[2] regulation and its successor that is often called eIDAS2 [3] (under development).

The term wallet is still ambivalent and is used with multiple adjectives, including 'identity', 'digital' and 'data' wallets. Consequently, there is no universal definition and understanding of digital wallets. To set a foundation for the remainder of this paper, we follow the working definition provided by the EU Architecture Reference Framework (Toolbox)[4] that states: *"An EUDI Wallet Solution is the entire product and service owned by an EUDI Wallet Provider, offered to all Users of that solution. An EUDI Wallet solution can be certified as being EUDI-compliant by a CAB"(p.9) . The objective of the EUDI-wallet is "to guarantee access to trusted digital identities for all Europeans allowing Users to be in control of their own online interactions and presence. It can be seen as a combination of several products and Trust Services that enables Users to securely request, obtain and store their information allowing them to access online services, present data about them and electronically sign or seal documents"(p.10).* Based on this definition we conclude that there are many functionalities to be developed and launched within a EUDI-wallet to provide a solution to responsible handling of personal data.

The definition of a digital identity wallet above highlights a couple of core functionalities that must be provided by a digital wallet. Getting all these functionalities in a data wallet that can be used for both public and private services is a new development with unprecedented digital service innovation opportunities. The EU Architecture Reference Framework recognizes multiple roles involved that could provide one of the required functionalities. Examples are public or private wallet service provider, public or private trust service provider, identity provider, attribute provider or technology

DGO 2023, July 11–14, 2023, Gdańsk, Poland

ACM ISBN 979-8-4007-0837-4/23/07.
https://doi.org/10.1145/3598469.3598501

[1]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[2]Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)
[3]Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281 final, 3.6.2021 (amendment on eIDAS).
[4]The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework, version 1.0, jan. 2023

provider. There are no off-the-shelf solutions available that satisfy all the legal requirements (section 4 provides an overview). Moreover, it is politically and technically unclear if and how a single wallet provider could or should provide all these functionalities, so collaboration to deliver these functionalities in a single wallet is therefore most likely needed.

Based on the evaluation of de eIDAS regulation[5], other non-academic literature and several initiatives that mostly failed, we expect that there are many barriers and a lack of guidance for design, development and launch of digital identity wallets provided by a public-private ecosystem. A Scopus search for academic literature on "Digital Identity Wallet" (in the Title, Keywords and Abstract) performed in January 2023 reveals just ten results. Most of the papers focus only on technological (security) aspects of digital identity management e.g. [6] and not on the social aspects. Therefore, we conclude that there is a lack of academic insights on socio-technical barriers when designing and launching digital identity wallets by a public-private ecosystem.

This paper contributes to understanding these barriers for digital identity wallets. In particular, we want to study the empirical barriers policy makers and aspiring wallet providers face at this stage. This requires a better understanding of the goals and requirements posed for wallets in Europe. Accordingly, the research question we focus on is twofold: (1) what are the main objectives and requirements for a digital identity wallet and (2) what barriers do actors encounter while trying to realize the objectives and requirements in practice? The European Digital Identity Wallet initiative provides a rich case for studying objectives, requirements and barriers.

This paper proceeds as follows: in section two we describe the research approach followed and limitations. In section three we draw on public service innovation literature as a theoretical lens to derive an initial set of expected barriers for the launch of digital identity wallets. Next, section four presents the European Digital Identity Wallet case study, setting the stage for analysing objectives and barriers. Section five reveals the results of two workshops with policy makers and (aspiring) wallet providers. We conclude with a section on the main conclusions and avenues for further research.

2 RESEARCH APPROACH

2.1 Case study design

To achieve the research objective, this paper draws on a single case study design with embedded multiple units of analysis. An embedded case study is a case study containing more than one sub-unit of analysis [7]. An embedded case study methodology provides a means of integrating quantitative and qualitative methods into a single research study. The main unit of analysis is the barriers for launching digital identity wallets (i.e. introducing operational wallets for use by citizens). The following three steps were employed for data collection.

First, we identified potential barriers that can be expected from public service innovation literature. The goal is to develop a shortlist of potential barriers that can be used as starting point for in depth discussions on empirical barriers during the workshops. Because the goal of this paper is to gain insights on the objectives and socio-technical barriers when designing and launching digital identity wallets, we chose the perspective of innovation and in particular public service innovation. Public service innovation is a concept that entails the implementation of a significant change in the way a public organisation operates or in the products it provides. Innovations comprise new or significant changes to services and goods, operational processes, organisational methods, or the way your organisation communicates with users (adopted from Cinar [8, p. 143]). The reason for using public service innovation is that digital identity wallets can be conceptualized as a means for public service innovation.

Second, we conducted a document review as part of the case study, focussing on the analysis of regulations to identify goals and requirements for digital identity wallets. Given the EUDI case study, we focus only on EU regulations. While there is no enforced EU regulation on digital identity wallets yet, we focus on preceding regulations that must be followed, regardless of the follow up regulation developed by the EU (i.e. the revision of the eIDAS act, also referred to as eIDAS 2). The preceding regulations for deriving goals and requirements are ECHR[6], ECFR[7], eIDAS and GDPR. Section four provides an overview of the main regulations and goals.

Third, we conducted two expert workshops in the Netherlands to identify barriers for launching digital identity wallets. The workshop designs were identical, the participants were different. Each workshop was an hour long. The first workshop was conducted on premise, the second workshop was done online, allowing a larger number of experts to participate. Participants were invited based on their demonstrated expertise in the area of digital identity management or personal data management. The experts invited could chose out of two workshops of one hour each, one workshop on site using Mentimeter and one workshop online using Microsoft Teams and Mentimeter (www.menti.com). After the two workshops the results were combined. In total 21 unique respondents participated in the workshops.

The first part of each workshop consisted of voting on 20 statements (agree/disagree), after which questions were asked after each statement about motivation and respondents could discuss with each other. These statements derived from the shortlist of potential barriers (see section 3). To make an inventory of which additional barriers were also recognized by respondents, based on their own experience and insights, the second part of the workshops asked participants to share using Mentimeter additional barriers that were not mentioned previously.

2.2 Limitations

There are three main limitations to this paper. First, the research is limited to the Dutch context of launching data wallets. The institutional, political, and cultural context in other countries may lead to a different set of relevant barriers. Second, the shortlist of barriers was formulated from the lens of public service innovation.

[5]Report From The Commission To The European Parliament And The Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) {SEC(2021) 229 final} - {SWD(2021) 130 final}

[6]European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf

[7]Charter of Fundamental Rights of the European Union, http://data.europa.eu/eli/treaty/char_2012/oj

Table 1: Categorization of barriers, based on Cinar [9]

Barrier type	Explanation	Examples
Organizational barriers	Linked to the internal context in which the innovation takes place	Administration of the innovation process activities, resistance or lack of support from specific actor(s), lack of available resources, rigid organizational structure/culture, lack of skills/knowledge/expertise
Interaction specific barriers	Related to the collaborative nature of this process and can be distinguished in the type of relation	Lack of shared understanding, lack of effective network governance, 'turf fights', lack of trust between organizations, lack of mutual benefits
Innovation characteristics related barriers	Innovative solution itself was perceived as a barrier by the member of the organization	Incompatibility, complexity, switching costs, lack of interoperability, platform/software problems and inflexibility
Contextual barriers	Linked to restrictions and obligations arising from laws and regulations	Restrictive tendering regulations, high costs to meet legal obligations, lack of standardization or geography
Barriers related to process stages	Barriers may vary according to the phases of the innovation process (idea generation and selection, development and design, implementation and sustainment)	Lack of available and accessible information on innovations elsewhere, unsystematic search, high levels of risk aversion, lack of resources and lack of an organizational learning culture, rigid organizational structure, top-down approach, ending of funding
Interrelations between barriers	Linked to the relationship between the barriers	Ongoing bad relationships between local governments lead to lack of shared understanding for the innovation collaboration, inappropriate framing contributed to public opposition

Other lenses, such as open innovation and the diffusion of innovation may have yielded other/additional barriers. Since the shortlist was decisive in the type of discussions during the workshops, we encourage the formulation of barriers based on other theoretical frameworks. Finally, we did not focus on the interrelations and interdependency between barriers, whilst they are expected to be important. Further research could provide a rich understanding of the various relationships and perhaps causalities between barriers.

3 THEORETICAL LENS

Our literature search for barriers centres on public service innovation literature. We conceptualise the design and launch of wallets in society as a public service innovation challenge, i.e. digital wallets are a means for public service innovation. For the purposes of this research we define *innovation* as *"a process through which new ideas, objects and practices are created, developed or reinvented, and which are new for the unit of adoption"* [9, p.264]. In order to identify potential public sector innovation barriers, it is important to understand the nature of public services and how public sector organisations innovate. Bloch [10] argues that three areas are important towards forming an understanding of how public sector organizations innovate: (a) the nature of public services themselves, (b) the context that public sector organizations operate within, and (c) the interfaces with other actors both within and beyond the public sector (i.e. the public-private ecosystem).

With respect to the interfaces Bloch [10] argues that a number of interfaces can be identified: (1) between the public sector and the private sector (including publicly owned enterprises); (2) between the public sector and citizens; (3) interfaces across governmental levels within the public sector, i.e. policy formulation, public administration and service production, (4) the interface between the various geographical levels of the public sector (i.e. local, regional, national) and (5) interfaces across different public domains, (e.g. health, education and defence).

Based on a systematic review of the empirical literature on barriers within public sector innovation processes, Cinar [9] distinguishes four types of barriers: (1) organizational barriers, (2) interaction specific barriers between innovation partners within the innovation process, (3) barriers related to perceived characteristics of innovation and (4) contextual barriers. Besides these types of barriers, Cinar [9] distinguishes also barriers related to process stages (5) and interrelations between barriers (6). These types are explained in more detail in table 1 below:

The categorization of barriers in Table 1 forms our theoretical lens and venture point for formulating more specific barriers that can be expected for the launch of wallets. Before formulating the more specific barriers (see Table 3), section 4 describes the EUDI case study that provides a context for interpreting the goals, requirements and barriers for data wallets.

4 EUDI WALLET ANALYSYS

4.1 Introduction of the EUDI wallet

The Briefing on the Revision of the eIDAS Regulation Findings[8] states that: "the eIDAS Regulation introduced the first cross-border framework for trusted digital identities and trust services, providing secure electronic interactions between citizens, business and public authorities. It sought to give EU citizens access to public services across the EU using electronic identification issued in their home country and recognized mutually by other Member States" (p.1).

[8]European Parliamentary Research Service, "Revision of the eIDAS Regulation, Findings on its implementation and application", march 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/ EPRS_BRI(2022)699491_EN.pdf

Governance: 1. National Accreditation Bodies 2. National Supervisory Bodies	
Supply: 1. Identity provider (eIDAS schemes) 2. Attribute providers (eIDAS schemes) 3. Qualified trust serive provider 4. Non-Qualified trust serive provider 5. Identity provider (non-eIDAS schemes) 6. Attribute provider (non-eIDAS schemes) 7. Technology Providers 8. Conformity Assessment body	Demand: 1. Citizens 2. Business 3. Public administration And 1. Public wallet service provider 2. Private wallet service provider 3. Public trust service provider 4. Private trust service provider 5. Online service providers (not-eIDAS)

Figure 1: Stakeholder roles in a wallet ecosystem

It continues with: "According to the Impact Assessment, the existing regulation: (1) Did not meet increased demand by public and private services for trusted identification and exchange of digital attributes. (2) Did not meet the current user expectations for seamless and trusted solutions to identify and share attributes across borders. (3) Available digital identity solutions were not able to address sufficiently the evolving data control and security concerns. (4) For trust services, the scope of the Regulation remained too limited and the lack of a level playing field across the EU hampered development of an internal market. Areas for improvement included national discrepancies on supervision procedures, diverging processes for remote identity proofing, and differences in conformity assessments." (p.7)

In response to these shortcomings mentioned, the European Commission proposed additional regulation of eIDAS. In the (proposed) amendment eIDAS (COM(2021) 281) the EUDI-wallet is introduced as one of the measures. This amendment is an extension on the existing eIDAS regulation (910/2014), therefore that is why both regulations will be combined in the further elaboration.

4.2 Stakeholders involved

Multiple functions are needed to deliver the service to citizens, business and public administration in accordance with the requirements mentioned above. These functions and roles could be provided by a single party, but it is more likely that providers will specialize and offer one or a few functions. Collaboration between different providers (both on the demand and supply side) then becomes necessary. In the Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework[9] (p.12) necessary roles are recognized and is spoken of a EUDI Wallet ecosystem. Figure 1 gives an overview of stakeholders in the ecosystem at the supply side, the demand side and governance:

Based on this inventory of roles and stakeholders, it can be established that multiple stakeholders are involved in providing the service to the citizen in the EUDI Wallet ecosystem.

[9]The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework, version 1.0, jan. 2023

4.3 Analysis of regulations

For the inventory of requirements for data wallets, we focus in this research on the regulations ECHR, ECFR, GDPR and eIDAS. Figure 2 provides a high-level overview of regulations, goals and functionalities.

First, article 8 (1) of the European Convention on Human Rights (ECHR) defines 'privacy' as an European fundamental right: 'everyone has the right to respect for his private and family life, his home and his correspondence'. The Charter of Fundamental Rights of the European Union (ECFR) regulates the 'protection of personal data' (as one of the components of guaranteeing privacy). In article 8 is stated that "everyone has the right to the protection of personal data concerning him or her" and that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". In addition to the fundamental rights, the principle of *proportionality* from Article 52 is also important as a requirement. This principle requires that any infringement on a fundamental right must be (1) in relation to the importance of the objective, (2) least far-reaching means (subsidiarity) and (3) suitable to achieve the goal.

Second, the General data protection regulation (GDPR) gives substance to the fundamental right to 'privacy' (rooted in the ECHR) and the 'protection of personal data' (rooted in the ECFR). The preamble of the GDPR states that "this Regulation respects all fundamental rights and observes the freedoms and principles recognized in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity." (p. 4).

Third, the proposed amendment of eIDAS explicitly refers to the GDPR and the European Digital Identity Wallet is introduced as a tool to enable the user to use and manage his or her personal data (article 6a(3). This amendment is an extension on the existing eIDAS regulation of 2014, therefore eIDAS describes goals and requirements for functionalities for:

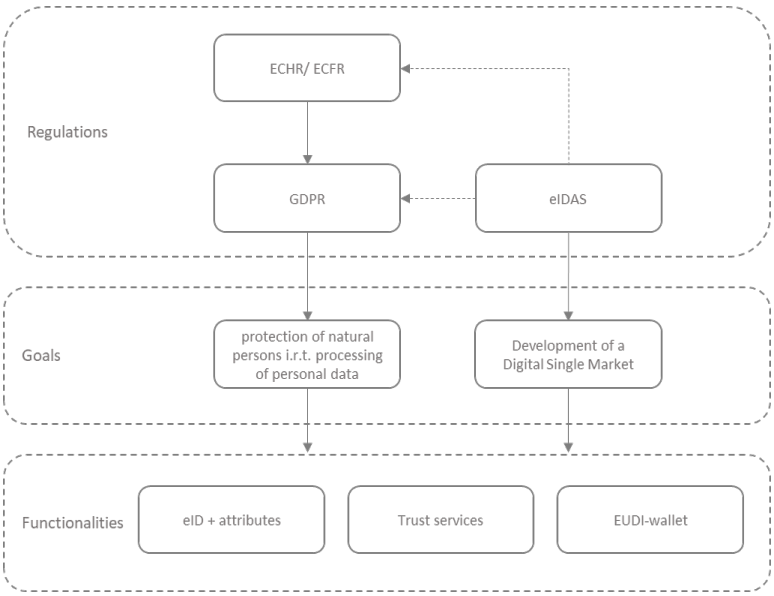

Figure 2: High-level overview of regulations, goals and functionalities

- an eID and the possibility to connect this eID with personal data (attributes),
- managing and sharing this personal data (with due observance of the rules from the GDPR),
- using trust services and
- the European Digital Identity Wallet

The preamble of the amendment of eIDAS states that "any personal data processing under this Regulation should be carried out in full compliance with the General Data Protection Regulation. In addition, this Regulation introduces specific data protection safeguards." (p.4). Therefore there is an explicit connection between eIDAS and GDPR, so the requirements from the General Data Protection Regulation are relevant to this subject. The preamble of eIDAS continues with: "to ensure a high level of security, the proposal is also consistent with Union policies related to cyber security. The proposal has been designed to reduce fragmentation applying the general cyber security requirements to trust service providers regulated by the eIDAS Regulation" (p. 4)

Starting at the bottom of figure 2 (functionalities derived from the goals) the analysis of the EU regulations reveals that the EUDI-wallet is an application that allows users to manage personal (eID) data (attributes) in a trusted way (called: trust services). This application combines and fulfils two objectives, namely (1) the contribution to the development of a Digital Single Market (rooted in eIDAS) and (2) the protection of natural persons in relation to the processing of personal data (rooted in GDPR). This relationship is further elaborated in the next sections.

4.4 Objectives and requirements found in GDPR

When it comes to personal data management, GDPR provides a set of principles and actions. Figure 3 provides an overview.

The GDPR starts with the statement "the protection of natural persons in relation to the processing of personal data is a fundamental right." This statement refers to Article 8(1) of the Charter of Fundamental Rights of the EU. Therefore, processing personal data must be lawfully, fairly and in a transparent manner. The objective of GDPR is to allow individuals to have better control of their personal data.

GDPR states in Article 5 (1a-1f) that the following principles must always apply to the processing of personal data: (1a) lawfulness, fairness and transparency, (1b) purpose limitation, (1c) data minimization, (1d) accuracy, (1e) storage limitation and (1f) integrity and confidentiality. Article 5(1b) states that personal data shall be collected for specified, explicit and legitimate purposes. These limited purposes are described in article 6 (1a-1f):

a. the data subject has given *consent* to the processing of his or her personal data for one or more specific purposes;
b. processing is *necessary for the performance of a contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c. processing is necessary for *compliance with a legal obligation* to which the controller is subject;
d. processing is necessary in order to *protect the vital interests* of the data subject or of another natural person;
e. processing is necessary for the performance of *a task carried out in the public interest* or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the *legitimate interests* pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

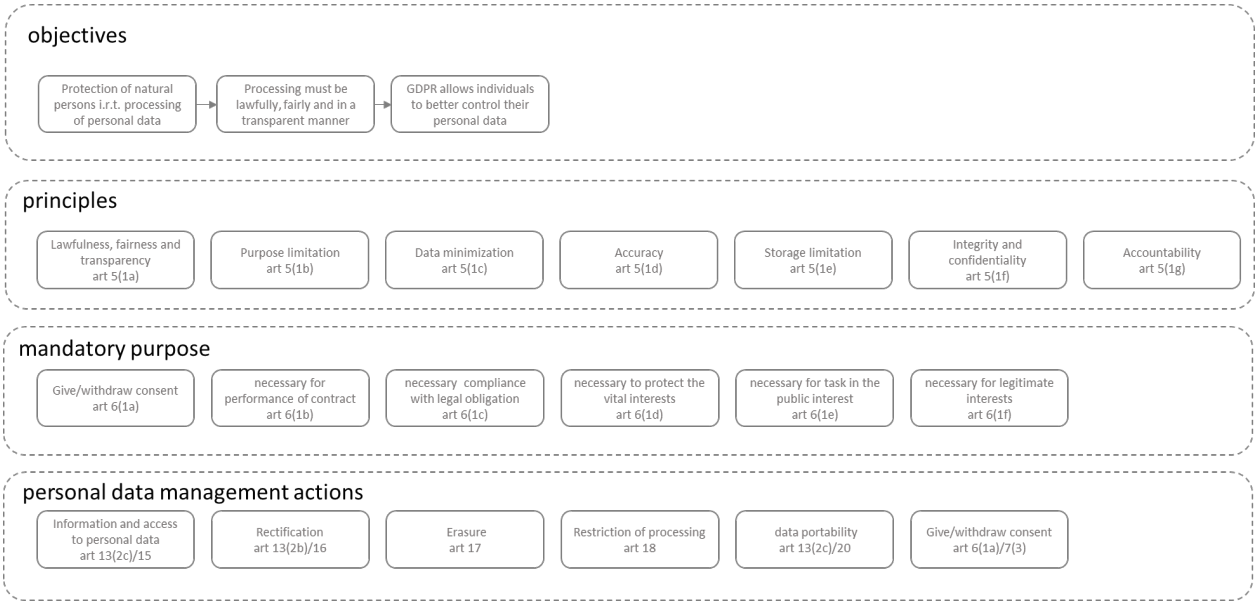

Figure 3: Objectives stated in GDPR

Table 2: Comparing general and specific eIDAS objectives

	eIDAS Regulation 2014, SWD(2012) 135	Amending proposal 2021, COM(2021) 281
General objective	*The development of a Digital Single Market; Stimulating and strengthening sustainable competition in the Digital Single Market; To promote the interest of consumers and to ensure high level of consumer protection for all EU citizens and businesses.*	*To ensure the proper functioning of the internal market, particularly in relation to the provision and use of cross-border and cross-sector public and private services relying on the availability and use of highly secure and trustworthy electronic identity solutions.*
Specific objectives	*Increase the availability of cross-border and cross-sector eIAS services and stimulate the take up of cross-border electronic transactions in all sectors (public and private); Ensure an optimal level and scope of governance; Ensure that competitive market developments are stimulated and that technological developments are not hindered in the eIAS market; Strengthen the competitiveness of the European industry and services sector; Ensure that all consumers can benefit from the advantages of (cross-border) eIDAS services.*	*Provide access to trusted and secure digital identity solutions that can be used across borders, meeting user expectations and market demand; Ensure that public and private services can rely on trusted and secure digital identity solutions across borders. Provide citizens full control of their personal data and assure their security when using digital identity solutions. Ensure equal conditions for the provision of qualified trust services in the EU and their acceptance.*

To effectively implement protection of a natural persons in relation to the processing of personal data, the natural person has the following personal data management actions at his disposal (described as: 'the right to'): (1) Information and access to personal data (art. 13/15), (2) Rectification, (3) Erasure, (4) Restriction of processing, (5) Data portability and (6) Give/withdraw consent.

4.5 Objectives and requirements in eIDAS

Where the objective of the GDPR is 'the protection of natural persons in relation to the processing of personal data', the general objective of the combination of eIDAS 2014 and 2021 is the development of a Digital Single Market through stimulating and strengthening sustainable competition, promoting interest of consumers and ensure high level of protection and highly secure and trustworthy electronic identity solutions [10] (p.7):

To achieve the goals, eIDAS gives three measures:

1. eID and the ability to link attributes (attestation) to this eID
2. trust services to enable honest and secure data exchange

[10] European Parliamentary Research Service, "Revision of the eIDAS Regulation, Findings on its implementation and application", march 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/ EPRS_BRI(2022)699491_EN.pdf

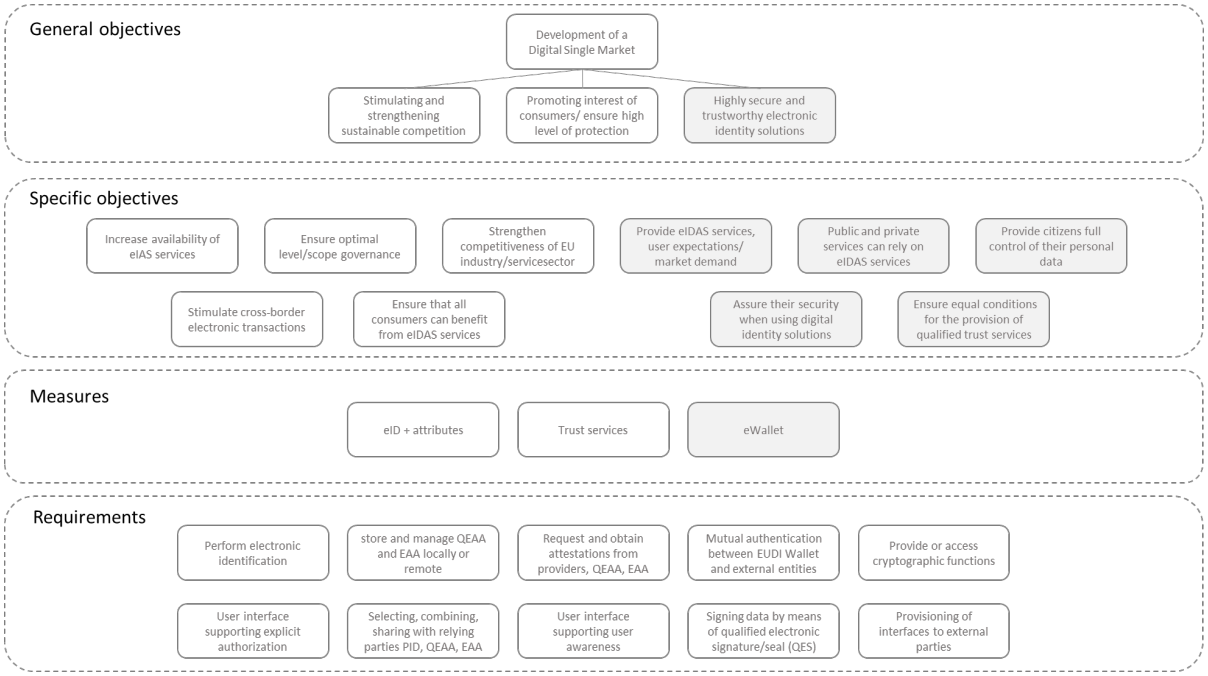

Figure 4: Overview of requirements in eIDAS

3. a data wallet (EUDI Wallet) to enable natural persons to manage their personal data

Figure 4 provides an overview of goals and requirements found in eIDAS (where the gray blocks refer to the amendment).

The Outline of the ARF[11] (p.25) describes the functional requirements of the EUDI Wallet as:

1. "Perform electronic identification, store and manage qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA) locally or remote;
2. Request and obtain from attestations from providers, qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA);
3. Provide or access cryptographic functions;
4. Mutual authentication between the EUDI Wallet and external entities;
5. Selecting, combining and sharing with relying parties PID, QEAA and EAA;
6. User interface supporting user awareness and explicit authorization mechanism;
7. Signing data by means of qualified electronic signature/seal (QES);
8. Provisioning of interfaces to external parties."

The Outline of the ARF (p.25) describes the non-functional requirements of the EUDI Wallet as:

1. "The EUDI Wallet shall meet the requirements set out in Article 8 of the eIDAS Regulation with regards to assurance level high.
2. As provided by the legislative proposal, EUDI Wallets shall be interoperable across the European Union and have externally oriented interfaces specified by common, technical standards.
3. The EUDI Wallet shall ensure full control of the user over their data held within their individual EUDI Wallet by integrating security and privacy by design.
4. The EUDI wallet shall have an easy to use interface and user experience and shall address accessibility, usability and inclusion.
5. The EUDI Wallet shall enable awareness of the user, and in particular allow the user to know when and how their EUDI Wallet is being or has been used, to be informed of the nature of all the operations carried on with their EUDI Wallet, and to present these elements in form of a history. In this context, the user shall also be notified of breaches of control, or be reasonably able to detect breaches of control.
6. The EUDI Wallet shall enable the user to share only the information they intend to share. The Wallet shall ensure an appropriate level of privacy, implementing policies about non-traceability and unlinkability of user's activities for third parties.
7. In order to bring trust to EUDI Wallet users and relying parties, conformity of the critical components of the implementations of the EUDI Wallet (including both the EUDI Wallet core functionalities and the implementation of interface protocols) shall be ensured by the EUDI Wallet issuer and confirmed by a recognized certification of the EUDI Wallet.

[11] European Digital Identity Architecture and Reference Framework-Outline, feb. 2022, https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

Table 3: Overview of workshop data analysis

	Barriers	Respondents	Totally agree	Agree	Neutral	Disagree	Totally disagree
1	There is no clear picture of what we mean by a data wallet.	21	10	8	1	1	1
2	Even with a data wallet, it is not always clear to citizens which data is shared for what and with whom	21	8	9	3	2	0
3	Citizens have no trust in private providers of data wallets	21	3	4	4	7	3
4	All personal data in one data wallet creates a security risk for the citizen	21	4	3	5	7	2
5	A strong growth in different (sectoral) data wallets causes confusion among end users	21	4	4	2	7	4
6	Little functionality (e.g. only storage of personal data) in the data wallet stands in the way of broad adoption	21	2	2	4	7	6
7	Vertical integration of data wallets will lead to monopolization	21	6	10	3	2	0
8	A data wallet costs more than it yields	21	0	3	8	3	7
9	Those who experience the benefits of data wallets often do not bear the burden	21	10	4	2	1	4
10	There is a lack of trust between stakeholders within the ecosystem	20	4	10	2	2	2
11	Difficult to start because a stable basis (rules, standardization etc.) is lacking	10	1	6	2	1	0
12	A data wallet from the government disrupts the market	10	3	3	1	3	0
13	Source holders (including software suppliers) develop their own data wallets outside the scheme	9	1	8	0	0	0
14	Legislation alone is not enough: data wallets also require other regulation.	10	7	2	0	1	0
15	Legislative alignment takes far too long, causing the development and adoption of data wallets to stagnate	10	3	5	1	1	0
16	There is a lack of standardization for exchanging data between data wallets.	8	0	2	1	3	2
17	Now regulating data wallets leads to stagnation of development	9	0	2	1	3	3
18	The roles of the government (of standard setter, source holder, verifier, market master) are too intertwined.	10	3	5	1	1	0
19	Due to a lack of shared vision within the government, there is a lack of coherent policies and measures	9	5	2	0	0	2
20	I do not have all the necessary knowledge to effectively fulfill my role in the development (or regulation) of data wallets.	9	1	2	3	1	2

8. The security of critical components integrated within the EUDI Wallet or used by the EUDI Wallet, which protect against misuse or alteration of identification data, authentication mechanism or consent mechanism shall be certified in accordance with the legal proposal.
9. In addition, the mechanism for relying parties to verify whether a EUDI Wallet used is genuine and certified, shall not enable the relying party to distinguish between two certified EUDI Wallets, in order to preserve the privacy of the user when performing pseudonymous authentication. Trust service providers shall not receive any information about the use of provided attestations.
10. The issuer of the EUDI Wallet shall not collect information about the use of the EUDI Wallet, which are not necessary for the provision of the EUDI Wallet services. In addition, the Wallet issuer shall not combine PID and any other personal data stored or relating to the use of the EUDI Wallet with personal data from any other services offered by this issuer or from third-party services, which are not necessary for the provision of the EUDI Wallet services, unless the user has expressly requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held."

4.6 Shortlist of expected barriers

In section 3 we identified the barrier types to be expected from public service innovation literature. We found that barriers can be distinguished into four types of barriers: (1) organizational barriers, (2) interaction specific barriers between innovation partners within the innovation process, (3) barriers related to perceived characteristics of innovation and (4) contextual barriers. Besides types of barriers there is also a relation between barriers related and process stages (5) and interrelations between barriers (6). In the sections 4.1 to 4.5 we analysed the regulations regarding the EUDI wallet to identify stakeholders, goals and requirements. Based on this analysis, we formulated a shortlist of expected barriers when developing and launching the EUDI wallet (see table 3). We have formulated several statements for each barrier type based on our own interpretation.

5 WORKSHOP RESULTS

5.1 Responses to the expected barriers

The first part of the workshops consisted of voting on 20 statements (agree/disagree), after which questions were asked after each statement about motivation and respondents could discuss with each other. To identify which barriers were also recognized by respondents (based on their own experience and insights), the second part consisted of entering them in Mentimeter. Table 3 provides an overview of statements and the aggregated responses from the workshop participants. Note that the number of responses in the second half of the statements is lower, because in one of the groups not all statements were treated due to time constraints.

Next, we briefly reflect on the level of agreement amongst participants. Most of the participants agreed with the first barrier, there is no clear picture of what a data wallet actually is. There was a discussion about the scope of 'data wallet': what exactly is meant by a data wallet?

The participants largely agreed with the second barrier. It is argued that this insight is necessary to give citizens confidence in the data wallet and its use. Legislation, quality marks, information, an independent supervisor, and even a digital forensic trace could be possible instruments.

Looking at the third barrier, the opinions of the participants are divided. It is argued that the situation is more nuanced: the Netherlands is a high trust society, in which, for example, there is more

trust in the medical doctor than in the government. Participants state that confidence in a public provider is high. It is also pointed out that citizens may not really trust private providers, but still use the service because they have no other choice.

When considering barrier #4, the opinions of the participants are divided. Central to the discussion is the question of whether risk relates to *storage* or *access to data*. That is an architectural issue. Storage can be both central and decentralized, but the degree of *access to that data* is considered to be decisive for the risk and not the place where it is stored.

Barrier #5 also shows divergence. A few participants argue that this is already the case: depending on the service and service provider (e.g. 'buying a house' or 'visiting the doctor'), different data wallets are available and citizens understand this difference and use different data wallets. Other participants argue that we are only at the beginning and that there are many more to come, so confusion is indeed lurking.

Most participants disagree on barrier #6. Some argued that the more functionality you put into a data wallet, the more complexity and therefore less adoption. Others argued that it is actually useful for a citizen to have for each life event a different data wallet.

The participants largely agreed with barrier #7. There was a discussion about the fact that, in addition to disadvantages such as higher (social) costs for end users, a monopoly can also have advantages such as lower coordination and transaction costs (for example, Dutch Railways and Itsme in Belgium), provided it is properly regulated.

The participants largely disagreed with barrier #8. There was some discussion about scope: what costs and benefits are included in the assessment?

Barrier #9 pulled together more agreement. The participants did point out that a misaligned business case is currently the case, but that this can be adjusted by correct pricing.

The participants largely agreed about barrier #10. Some participants pointed out that lack of trust depends also on the number and type of stakeholders involved within the ecosystem. If there are only a few parties who know each other, trust quickly builds. This is more difficult if many parties are involved who also do not know each other very well.

The participants largely agreed with that there is a lack of standardization (barrier #11). Some participants did indicate that this also offers opportunities to start something new. Others also pointed to the investment uncertainty because it is not clear whether and how the government will regulate.

When considering barrier #12, the participants largely agreed with this statement that a wallet provided by the government would disrupt market development for wallets. Several participants did state that the government should adhere to the same rules, so that a level playing field is created. Another pointed out that there are groups of citizens from whom there is less money to earn, so it is good that the government makes a data wallet available for free.

Barrier #13 was generally agreed upon. Participants expect a wide variety of wallets offered. Whether the wallets will comply with the establish regulations is a huge concern.

Looking at barrier #14, most of the participants agreed that more is needed than (European) legalisation for a healthy wallet ecosystem. Other forms of regulation that provide a mix of incentives is needed.

Most participants agreed on barrier #15. Participants indicated that it is not a problem to wait for careful legislation, but parties are waiting due to the lack of clarity. It was also noted that a system of agreements does not require separate legislation, so that parties can already regulate their cooperation.

There was general disagreement on barrier #16. There was a discussion about semantics: there are many standards available for exchanging data, but adoption (standardization) is lagging. Moreover, the discussion here zoomed in on the lack of boundary resources in the wallet ecosystem. Here, boundary resources refer to a wide area of standards, tools, methods, procedures and decision-making structures that actors can collaborate with. A key question is who (public or market actors) should be in the lead when it comes to the development and governance of boundary resources.

When it comes to the timing for regulating data wallets (barrier #17), there is no consensus. In the discussion, a distinction was made between the phase of market development and the phase of market regulation. Some participants stated that the market development phase has been completed and we have now entered the market regulation phase. Regulation is therefore desirable. Others stated that we are still in the market development phase and that regulation is not yet desirable. It was also noted that there is too little knowledge to regulate effectively.

Most participants agreed that the roles of public agencies are currently too intertwined (barrier #18). Currently, governments play multiple roles, including policymaking, data provider, service provider, potential wallet provider and regulator.

The participants largely agreed with the lack of a collective vision within the Dutch government (barrier #19). Currently, multiple government agencies have different policy directions regarding wallets and personal data management. This hampers market investments.

Finally, the participants were much divided on the barrier #20, which zooms in on the knowledge required. Some stated that data wallets are complex where a lot of different knowledge is needed, especially when it comes to social impact (behaviour, psychology). Others argued that there was sufficient technical knowledge.

5.2 Additional barriers mentioned in the workshops

In the second part of the workshops, participants were asked what additional other barriers they see for the launch of digital wallets. Table 4 provides an overview of the additional barriers mentioned by the participants. The type of barrier and ordering is added later by the researchers, in line with the types explained in section 3.

Looking at the additional barriers listed in Table 4, we observe that:

1. Participants supplemented the list of 20 expected barriers with 30 additional barriers. That is more than we expected.
2. The 30 additional barriers included: 3 contextual, 9 innovation characteristics related, 15 interaction-specific, 3 process stages barriers.
3. There were no organizational barriers mentioned.

Table 4: Additional barriers identified during the workshops

Additional barrier mentioned by workshop participants	Type
The low level of cooperation and distance/misalignment between and with EU legislation and Dutch policies.	Contextual barriers
Geopolitical interests and influences could become more decisive in this domain as well (e.g. the launch of an Apple Data Wallet in the EU).	Contextual barriers
Differences in the regulation of wallets, issuers, controllers, and other parties across EU member states impedes the formation of a level playing field.	Contextual barriers
Digital readiness of citizens, some groups will have difficulties to wield wallets. This raises concerns regarding digital inclusion and representation.	Innovation characteristics related barriers
Many public and private data sources are not yet accessible for (private sector) data wallets. There is still little data from the entire ecosystem, now all kinds of tricks (e.g. screen scrapping) are used to fill the wallet.	Innovation characteristics related barriers
The lack of boundary resources that promote interoperability in the wallet ecosystem (databases, API, data specifications, hardware, software etc.). Without these, we cannot fill the wallets with useful and high quality data and functionalities.	Innovation characteristics related barriers
Limited adoption of suitable smartphones. Many older smartphones with older versions of iOS and Android do not satisfy some of the ETSI hardware security requirements.	Innovation characteristics related barriers
Digital identity matching is a major challenge for commercial service providers, since they are not permitted to use the unique public citizen identifier (Burger Service Nummer, BSN). We lack a unique and persistent (EU) citizen identifier that can be used by public and private parties.	Innovation characteristics related barriers
Dependence on mobile devices as platform and gateway for wallets.	Innovation characteristics related barriers
Overview for citizens when/which data has been shared with actors and for what purpose. There must be one mandatory place for that, mandated by the government.	Innovation characteristics related barriers
Too much focus on regulating wallet suppliers instead of building standards and boundary resources (e.g. APIs and shared data models).	Innovation characteristics related barriers
The Dutch government focusses too much on open source requirements for wallets, it is not clear which components of wallets should be open source.	Innovation characteristics related barriers
There is no national wallet rollout strategy for the Netherlands.	Interaction-specific barriers
Slow decision making regarding 'acceptable' cost and revenue models for wallet services and data exchange.	Interaction-specific barriers
Public opinion and distrust, no free choice for individual, image of a mandatory use of wallets, similar to COVID 19 QR codes.	Interaction-specific barriers
The difference between attribute issuers and wallet providers is not well enough understood.	Interaction-specific barriers
Lack of mutual understanding about the desired results when using a data wallet.	Interaction-specific barriers
The regulating parties lacks the knowledge and competences to understand specific risks related to wallets is and is therefore unable to weigh up regulatory actions.	Interaction-specific barriers
Distrust from the Second Chamber of the Dutch Parliament is also about (lack of) knowledge.	Interaction-specific barriers
The First Chamber/Senate is delaying relevant national regulation.	Interaction-specific barriers
Lack of the nationwide adoption and implementation of a 'qualified high-level of assurance' digital identity as a mandatory component of wallets.	Interaction-specific barriers
Fragmented innovation landscape: there are far too many loose-coupled and overlapping initiatives (let all the flowers bloom).	Interaction-specific barriers
No administrative level urgency and priority to make data available to data wallets.	Interaction-specific barriers
Fuzziness surrounding 'wallet ethics'. For instance regarding privacy, transparency and freedom of choice for wallet users in every context (guarantee public values, even without a wallet).	Interaction-specific barriers
Political bias towards personal data management and wallets (not choosing the most rational solution, but choosing the politically feasible one).	Interaction-specific barriers
Multiplicity of actors -> traceability when things go wrong somewhere in the data chain.	Interaction-specific barriers
The number of agreements that must be in place is overwhelming.	Interaction-specific barriers
The need for online/mobile on boarding of users scares off certain service providers.	Process stages and barriers
The usefulness for the citizen/end user is not very clear, making it difficult to develop business models with a long term viability.	Process stages and barriers
Lack of good use cases for launching digital identity wallets. There is no killer use case. What can you do more than, for example, show your ID?	Process stages and barriers

4. The contextual barriers mainly refer to legal issues such as the lack of a level playing field due to differences in legislation.
5. Innovation-related barriers mainly relate to the lack of knowledge on the part of the user, the lack of access to data and problems arising from the combination of hardware and software. One could argue that these types of barriers are mostly related to the process stage development and design.
6. Interaction-specific barriers mainly relate to the lack of effective network governance: timely discussions, lack of mutual understanding and lack of trust.
7. The lack of benefits and use cases for citizens is a type of barrier that relates mainly to the process stages implementation.

These observations provide directions for further research. The following section provides an overview.

6 CONCLUSION AND DISCUSSION

The main goal of this paper is to contribute to the understanding of the goals, requirements and barriers behind digital identity wallets. The research question is twofold: (1) what are the main objectives and requirements for a digital identity wallet and (2) what barriers do actors encounter while trying to realize the objectives and requirements in practice?

In section 4 we answered question 1 as follows: the main objectives of the EUDI wallet is the contribution to the development of a Digital Single Market through stimulating and strengthening sustainable competition, promoting the interest of consumers and ensure high level of protection and highly secure and trustworthy electronic identity solutions.

The main requirements of the EUDI Wallet include performing electronic identification, store and manage qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA) locally or remote, providing access to cryptographic functions, enable mutual authentication between the EUDI Wallet and external entities and providing interfaces to external parties.

The barriers actors encounter while trying to realize the objectives and requirements in practice are numerous and multi-faceted. The shortlist of expected barriers inspired by literature on public service innovation proved to be a good starting point for discussions with experts. However, not all experts agreed on the definition and relevance of the expected barriers presented to them during the workshops. A possible explanation could be the heterogeneity of perspectives of the participants: different barriers can be experienced from a public policy making perspective compared to a commercial wallet provider perspective. Moreover, the same barrier can be experienced differently from the government perspective than from a private perspective. An example is the discussion that followed after the statement that 'citizens have no trust in private providers of data wallets'. The workshops also revealed an additional set of barriers that were not expected from a public service innovation perspective. Based on the responses of the respondents, we can conclude that barriers for launching digital identity wallets by a public-private ecosystem are mostly interaction-specific and technical innovation characteristics related barriers. With reference to the characterization of interfaces, as mentioned in section 3, the interaction-specific barriers can be mainly related to the interfaces between the public sector and the private sector. Policy makers looking to stimulate the launch of digital wallets must focus on removing these different types of barriers.

This research is the first to perform a systematic identification of requirements and barriers for digital wallets. Given the societal impact of these wallets, more research is encouraged. In particular, we identify three main research directions. First, there might be a relationship or hierarchy between barriers. Finding the relationships can perhaps reveal path dependencies between barriers, and help weigh prioritize which barriers should be addressed first. Second, there is need for academically grounded studies on effective solutions for the barriers. Which policy instruments and regulatory tools can be used to effectively address the specific challenges? Finally, we need to look beyond the current phase of wallet development, which can also be considered as the innovation and market development phase. The next phase will be the widespread use of wallets for all kinds of use cases spanning the public and the private sector. If the ambition of the new eIDAS regulation is realised, citizens will be able to choose from a spectrum of different wallet providers, each offering different customer journeys across multiple domains (i.e. government, banking, insurance, mortgages, health, mobility, energy etc.). Wallets have the potential to become 'Superapps', a one stop shop for many if not all citizen-to-government or citizen-to-business interactions. We can expect all sorts of new challenges from a policy, economic and even ethical perspective. This phase will reveal gaps in current regulations, standards and governance models and require more market regulation. Future research is needed on how to effectively regulate digital wallets and safeguard public values.

REFERENCES

[1] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz, "A taxonomy for privacy enhancing technologies," *Comput Secur*, vol. 53, pp. 1–17, 2015, doi: 10.1016/J.COSE.2015.05.002.
[2] J. Priisalu and R. Ottis, "Personal control of privacy and data: Estonian experience," *Health Technol (Berl)*, vol. 7, no. 4, pp. 441–451, 2017, doi: 10.1007/s12553-017-0195-1.
[3] N. Bharosa, S. Luitjens, R. Van Wijk, and T. Pardo, "Panel: Removing the barriers for personal data management," in *ACM International Conference Proceeding Series*, May 2018. doi: 10.1145/3209281.3209327.
[4] D. E. 3rd and T. Goldstein, "ECML v1.1: Field Specifications for E-Commerce," Apr. 2001, doi: 10.17487/RFC3106.
[5] "Digital Wallets: An Introduction." https://www.gartner.com/en/documents/308109 (accessed Jan. 27, 2023).
[6] A. Enge, A. Satybaldy, and M. Nowostawski, "An offline mobile access control system based on self-sovereign identity standards," *Computer Networks*, vol. 219, no. 109434, 2022.
[7] R. K. Yin, *Case Study Research and Applications: Design and Methods*, 6th ed. Thousand Oaks, CA: SAGE Publications, 2018.
[8] E. Cinar, C. Simms, P. Trott, and M. A. Demircioglu, "Public sector innovation in context: A comparative study of innovation types," *Public Management Review*, 2022, doi: 10.1080/14719037.2022.2080860.
[9] E. Cinar, P. Trott, and C. Simms, "A systematic review of barriers to public sector innovation process," *Public Management Review*, vol. 21, no. 2, pp. 264–290, 2019, doi: 10.1080/14719037.2018.1473477.
[10] C. Bloch and M. M. Bugge, "Public sector innovation-From theory to measurement," *Structural Change and Economic Dynamics*, vol. 27, pp. 133–145, 2013, doi: 10.1016/J.STRUECO.2013.06.008.