Yiğit Aşkan

Digital Credentials in your Wallet: A Design Knowledge approach to European Digital Identity Framework governance for public sector organizations

Master Thesis

at the Chair for Information Systems and Information Management
(Westfälische Wilhelms-Universität, Münster)

Supervisor: Prof. Dr. Tobias Brandt
Tutor: David Nowak, M.Sc.

Presented by: Yiğit Aşkan

Date of Submission: 2025-06-16

Table of Contents

Figures

Tables

Abbreviations

ARF	Architecture and Reference Framework
EAA	Electronic Attestations of Attributes
eIDAS	Electronic Identification, Authentication and Trust Services
eIDMS	Electronic Identity Management System
EUDI	European Union Digital Identity
EUDIF	European Union Digital Identity Framework
EUDIW	European Union Digital Identity Wallet
IT	Information Technology
ITG	Information Technology Governance
KYC	Know Your Customer
PbD	Privacy-by-Design
PKI	Public Key Cryptography
Pub-EAA	Public sector Electronic Attestations of Attributes
RP	Relying Party
SSI	Self-Sovereign Identity
TSP	Trust Service Provider
VC	Verifiable Credential
(Q)EAA	Qualified Electronic Attestations of Attributes
(Q)TSP	Qualified Trust Service Provider

1 Abstract

Digital Identity Wallets have been gaining traction in the European Union as a secure, widely accepted, and interoperable electronic identification and data sharing means for natural and legal persons. Adoption of the European Digital Identity Framework Regulation in 2024 gave European public sector organizations and select private sector organizations an obligation to adopt European Digital Identity Wallet use cases by the end of 2026. This thesis addresses knowledge and practice gaps concerning the adoption of digital identity wallets in the European public sector. Previous research shows that adoption and value realization of digital identity means in the European public sector requires context-aware governance strategies that support organizational capacity to create value through the implementation of digital identity solutions. However, findings from the literature suggest that such governance strategies have failed to materialize during the implementation of eIDAS (Electronic Identification, Authentication and Trust Services) Regulation from 2014 onwards. We conducted a design science research study to develop an intra-organizational digital identity wallet governance model artifact for public sector organizations that identifies key activities, controls, constraints, and workflows towards creating organizational value using digital identity wallets. We evaluated the model artifact with 28 semi-structured interviews attended by domain experts representing public and private sector organizations. Through expert evaluation, we found that our model identifies the organizational adoption and implementation context correctly and proposes suitable governance controls. Using Information Technology Governance (ITG) modelling frameworks, we demonstrate barriers, drivers, and adoption antecedents of digital identity wallets in an IT governance modelling context to embed EU Digital Identity Wallet value conceptualizations in public sector business processes and service design.

Keywords: European Digital Identity Wallet, digital identity, eIDAS, information technology governance, public sector, model

2 Introduction

Citizen identities have always been at the core of public service delivery processes since the advent of modern bureaucracies. Nowadays, ICT-capable governments collect, process, and rely on digitalized citizen identities to fulfill their mandates. ICT-enabled processing capabilities made it possible for governments to experiment with and roll out new digital trust concepts. (A. M. B. Lips et al., 2009) Concepts such as electronic signing enable document signing to be done in electronic environments. Use of Public Key Cryptography (PKI) and electronic signature certificates in government processes enables the recognition of electronic signatures with legal value in EU Member States as early as the 2000s, with the adoption of the Electronic Signatures Directive of 1999/93/EC. (European Commission, 1999) The use of electronic signatures within Member States has enabled digital means to interact with public services. For example, instead of relying on the circulation of paper documents, electronically signed documents were notified to clients and other authorities, which could be checked for authenticity based on the electronic document's signature value. (Reichstädter, 2003) It was also possible to make use of cryptographic elements to generate pseudonyms, assign pseudonymous connection values to data attributes generated throughout service delivery processes to the citizen's national identity. (Reichstädter, 2003) State-issued digital identification schemes in the EU have begun to provide citizens with signing certificates in a secure environment within an identity card or an online environment as early as the 2000s. (Shehu et al., 2019) Use of these certificates enabled citizens to authenticate themselves to online service portals that are often maintained in conjunction with e-government initiatives. (Shehu et al., 2019) Furthermore, electronically sign documents. (Shehu et al., 2019) Although applications of computational cryptography had ushered in novel technical concepts towards public digital services, their conceptual premise largely rested on long-established concepts of tripartite trust relationships, involving issuers, relying parties, and neutral third parties offering oversight functions. (Sharma & Mishra, 2011) As a result, fundamental concepts of trust have not been transformed but rather computerized and remediated through digital interfaces. (Bodó, 2021; Ishmaev, 2021) Moreover, it is being practiced with increasing frequency through public digital service channels for citizen interactions. (Whitley & Schoemaker, 2022)

National citizen identity management practices have certainly not developed in a vacuum. Each European state has developed individual, organizational, and system-level

perceptions that may be linked to societal expectations and administrative path dependencies. One salient debate is the controllability of personal data vis-à-vis the large-scale rollout of digital public identity systems, as datafication of personal identity has been a salient concern. (Sroor et al., 2022) European states have historically had abundant reasons on the individual level to develop skepticism towards the rollout of state-backed identification schemes (Michael & Michael, 2006). Tied to this aspect is the incorporation of increasingly sensitive personal attributes to public digital identity artifacts. (A. M. B. Lips et al., 2009) This not only spurs the possibility of misuse and fraud by third parties but also the possibility of misuse by the very entity that supplies the technical capability. (Giannopoulou, 2023a; Michael & Michael, 2006; Whitley & Schoemaker, 2022) The collectivization of personal identities by governing powers might result in the loss of personal agency over citizen-government relationships. (Michael & Michael, 2006) In contrast, the digitization of identity management enabled new ways of public service delivery towards citizens, the introduction of which may be perceived as opportunities by the government, as the concept went hand in hand with promises of improved efficiency and effectiveness in service provision, information security, convenience, and access. (Giannopoulou, 2023a; A. M. B. Lips et al., 2009) Moreover, the datafication of personal attributes in government processes has introduced access control management. To public services, extending its scope (Giannopoulou, 2023b). This fusion of authentication and authorization is significant as digitally mediated services nowadays carry the capability to both identify and authorize the release of public services to citizens simultaneously based on their identity attributes. (Sroor et al., 2022) Scholars reported another dimension of the debate over state-level path dependency that extends the outlook over the historical development of state identity management practices and structural peculiarities of European states, such as multi-level political governance. For example, it has been suggested that high levels of trust for and acceptance of social welfare state functions might drive positive attitude formation in citizens. (Pouloudi & Kalliamvakou, 2011; Weigl et al., 2023) Various other features of a Member State's digital identity management practices have been found to carry detrimental effects. Availability and useability of a national digital identities from a user experience perspective might enable digital identities to be use case drivers for citizen to government interactions rather than acting as digital gatekeepers to public services (Pouloudi & Kalliamvakou, 2011) efforts to establish trust, transparency and accountability in citizen to government identity data transactions might help drive individual acceptation factors (Pouloudi & Kalliamvakou,

2011) However, trust building activities and system design considerations alone might not be enough to account for structural factors. European states with strong federalist traditions might have clear structural dependencies that might resist centralization of identity attributes and centralized methods of public digital identity service provision. (Pouloudi & Kalliamvakou, 2011) Furthermore, it is possible for individual attitudes around identity management practices to be formed over historical learnings. Individuals might tend to question the credibility and trustworthiness of the citizen-government digital relationships. In such cases, concerns over individual agency and privacy might trump implementation priorities. (Pouloudi & Kalliamvakou, 2011) From the perspective of implementors, standardization of data models in identity attributes might alleviate concerns over interoperability, and standardization of unique and persistent identifiers for citizens might even lessen interoperability challenges even more. However, in certain European states, legislative frameworks may resist such standardization initiatives. (Pouloudi & Kalliamvakou, 2011) Such legal frameworks might have been formed by national consensus to limit the centralization of identity attributes. (Pouloudi & Kalliamvakou, 2011) Alternatively, as a response to privacy concerns (Kubicek & Noack, 2010) or as a result of institutionalized trust relationships in existing centralized structures to manage identification data and personal attributes, regardless of whether such organizations are public or private in functionality. (Kubicek & Noack, 2010) Learnings from member states might suggest that a pan-European identity management strategy is a challenging task that exists in local historical and sociocultural contexts in its implementation and stakeholder relationships, especially within member states that have established multi-level governance structures with clear responsibility delineation. (Pouloudi & Kalliamvakou, 2011) In short, digital identity management practices do not evolve in vacuums. They are interlinked to socio-political playing field (Giannopoulou, 2023b; Whitley & Schoemaker, 2022) owing their design principles, (Whitley & Schoemaker, 2022) stakeholder structures, (Giannopoulou, 2023b; Kubicek & Noack, 2010) commercial models (Degen & Teubner, 2024) and governance systems with associated incentive structures. (A. M. B. Lips et al., 2009) to the context in which they have been developed and have been launched.

These factors have not spared the success of pan-European standardization initiatives. Following widespread provisioning of digital public services around the European Union, access to public services meant having access to stable and recognized identifiers for

citizens of provisioning countries as well as citizens of other Member States who exercised their fundamental right to access cross-border public services. As the European Union progresses towards common goals to establish a Single Digital Market, where European citizens are empowered to seamlessly live, study, and work across internal borders, cross-border digital public services have started to be enacted in cooperation with different Member States. Reducing access barriers to such services meant a pan-European initiative to standardize and prescribe a digital trust framework for European credential holders to interact with digital public services, across borders, securely. (European Commission, 2022) Subsequently, the European community has introduced the Single Digital Gateway (SDGR) and eIDAS Regulations, motivated by an increase in cross-border service clientele and common policy goals. Researchers posit that the governance challenge of pan-European identity initiatives has not been solved yet. (S. Lips et al., 2020) The landscape is complex with differing stakeholder needs (Weigl & Reysner, 2024), interoperability problems on different levels (Hölbl et al., 2023), and implementation initiatives falling short of expectations in terms of generating public value through enacted technologies (Ramona, 2021)

Aside from service access, over the past decade, personal data has been a contested concept in terms of data controllability and proper usage, (Weigl & Reysner, 2024) leading towards more awareness, critical discussion and action from policymakers, (Weigl et al., 2022; Weigl & Reysner, 2024) individuals and technologists.(Cap & Maibaum, 2001; Shoshana, 2015; Whitley & Schoemaker, 2022) As European state identity management practices have evolved alongside individual and institutional perceptions about the woes of datafication, centralization, and technical promises for data sovereignty, the concept of digital identity wallets has come to the fore. These digital identity wallets enable personal data control for the holder of digital identity documents and credentials. (Lukkien et al., 2023) So much so that they have earned the spotlight in the flagship initiative of the European Digital Identity Framework (EUDIF). The framework promises to introduce a comprehensive update to pan-European recognition of cross-border personal identification. The digital identity wallet and its related components are selected to chart a pathway beyond the current challenges of the European electronic identification infrastructure. It is important to note that, however, EUDIF will act as a scope extender on top of the earlier eIDAS Regulation and Single Digital Gateway Regulation, with its recognition of data sharing possibilities in a recognized and trusted

multi-actor environment. (Lukkien et al., 2023) Inevitably, like its predecessor, the EUDIF will face governance challenges from a multitude of perspectives that may need addressing throughout its implementation cycle. As we discussed in this chapter, state identification is not exempt from contestation from the needs and expectations of different stakeholders, values, and beliefs of institutions regarding the scope and purpose of digital identity projects.

2.1 Problem statement

We derive several conceptual-level and governance-level challenges associated with the introduction of the EUDIF Regulation by the European Commission that will form the basis of our problem statement and, henceforth, our problem formulation process. Initially, the adoption of the European Digital Identity Framework (EUDIF) in 2024 has started the clock on several Commission Implementing Regulations (CIRs) that are meant to define mandated actions of concrete implementation of the regulatory governance framework. (European Commission, 2024) As a result of EUDIF's adoption, Member States have a concrete and urgent obligation and a deadline until the end of 2026 to: (1) develop, notify, and deliver a compliant digital identity wallet solution to every citizen who wishes to use it. (2) Adopt compliant and notified digital identity wallets as a valid method for conducting digital transactions in public sector service delivery processes and use cases. Furthermore, the obligation to adopt compliant and notified digital identity wallets also extends to select private sector entities that were deemed by the regulation to fulfil critical socio-technical functions. (European Commission, 2024) Secondly, the EUDIF Regulation enumerates in the wallets' definition, along with several technical specifications, several values and principles such as enabling control over one's data, facilitating user privacy preservation, and data sovereignty. However, EUDIF does not provide contextualization of such values and principles in a public sector perspective, leaving their interpretation open-ended to sectoral practitioners. Moreover, the EUDIF ascribes several conceptual values to the digital identity wallet, but such attachments of value are also never contextualized from a sectoral point of view. For example, the Architecture and Reference Framework (ARF) is developed by the European Commission as the blueprint for the implementation of the technical, legal, and governance components recognized by the EUDIF regulation. ARF recognizes the EUDI initiative as an 'ecosystem' of digital identities, while the regulation does not explicitly propose such a definition.

Based on what we derived from the practical problem space, we observe that among pressing deadlines for wallet development and adoption by the public sector, conceptual ambiguity that the researchers have demonstrated. (Lukkien et al., 2023) and attribution of value and principles on the enactment of technical artifacts in an evolving digital ecosystem presents a salient governance gap for this thesis to address. It has been suggested that the initial wave of regulatory frameworks for cross-border identification and data sharing has had persistent challenges in implementation that are underpinned mainly by governance shortcomings. (Leosk et al., 2021; S. Lips et al., 2020) We can suggest that similar governance challenges may arise during EUDIF implementation. Recognition of the EUDI initiative as an ecosystem extends the inquiry into an ecosystem governance lens where recognized actors should harness the capabilities of the newly developing ecosystem to create value; however, in the case of EUDIF, the methods and objectives of value creation have not been made clear in the literature or the regulatory framework. We can also suggest that the modes of value creation in a multi-stakeholder ecosystem are underpinned by the governance design of the ecosystem and participant capabilities to create collaborative value.

EUDIF indirectly attributes various themes to digital identity wallets. By recognizing digital identity wallets as a method of interfacing with public and private organizations, the wallet is elevated to a service delivery means status as well as a public service offering. Moreover, data sharing capabilities of a digital identity wallet rest upon authentic data points supplied by the controllers of authentic data sources that are primarily public sector organizations, essentially creating a multi-sided public service platform ecosystem. (G. Parker et al., 2017) On top of a pan-European public digital ecosystem, the digital identity wallet is situated as the primary digital platform for service delivery for clients. This mass introduction of related concepts has not transpired into academic attention and scrutiny in the existing literature. We suggest the need to discover essential value creation methods and mechanisms. We posit that value creation may happen in multi-level settings where public and private organizations need to collaborate to create ecosystem value. From this position, discovering critical links, barriers, and drivers for ecosystem participation may be especially helpful to inform practical governance challenges.

Thirdly, we observe that the obligation to adopt and therefore participate in the ecosystem involves the need for a systematic understanding of how public sector organizations can

create value by participating in the EUDI ecosystem. Ecosystem participation has been marked with compliance requirements and essential barriers by the EUDIF Regulation (European Commission, 2024), thus necessitating a hierarchy of challenges to achieve full ecosystem participation. For example, without compliance with fundamental ecosystem requirements, an entity may not enrol as a wallet relying party or data producer; from this dimension, it is possible to indicate a 'readiness' challenge that is underpinned by compliance with technical specifications. Lastly, we argue that ascribing specific values and principles to the digital identity wallet necessitates scrutiny to discover methods for their operationalization in sectoral contexts. As scholars demonstrated, state digital identity management practices are not value agnostic but relatively path dependent and conducive to adopting the values of operators. Thus, contextualization of ascribed values may enable the creation of public value through service delivery moving forward.

Having observed the problem space, we propose a design knowledge approach to EUDIF governance towards public sector organizations. Our thesis follows the seminal Design Science Research (DSR) methodology introduced by Peffers, (Peffers et al., 2007) and supplemented by other scholars (Hevner et al., 2020) and presented in adapted detail by (Brocke et al., 2020) To offer a design knowledge approach towards the observed EUDIF governance challenges in public sector organizations. We will attempt to systematically acquire design knowledge on practical governance challenges experienced by European public sector institutions as they get ready to implement the EUDIF Regulation and adopt EUDIWs. To this end, we have held 28 interviews with domain experts, representing public and private sector organizations in two evaluation phases. Our study follows the DSRM iteration cycle proposed by (Peffers et al., 2007) through which we have obtained a preliminary set of design objectives towards designing an intra-organizational EUDIF governance model. We evaluated this set with 18 expert interviews to arrive at the first iteration of the designed governance model artifact. Afterwards, we have conducted 10 expert interviews to derive suitable improvements towards the first iteration. Finally, we present to the reader the second iteration of the governance model artifact and offer a discussion on its use implications for public sector organizations.

2.2 Research motivation

We derive motivation to carry out our research based on the practical problem space. (Peffers et al., 2007) Furthermore, to establish further relevancy and formulate our research questions, we derive additional motivational bases from concrete gaps in the digital identity research domain.

Firstly, scholars suggest that the ecosystem perspective introduced by the Regulation necessitates a wide range of new government capabilities. (Degen & Teubner, 2024) The intertwined nature of digital identity wallet ecosystems' technology and governance. (Kölbel et al., 2022) they also identify specific capabilities tied to creation of legitimacy, accountability and effectiveness to generate increased public value in ecosystems (Degen & Teubner, 2024) The formulation of the European Digital Identity Wallet project have been found to be tied to terminologies such as 'digital sovereignty', 'privacy', 'data control' and 'rule setting for gate keepers to information, ensuring transparency behaviour and accountability' (Weigl et al., 2022) From an institutional perspective on trust, it has been suggested that trust building has specific linkages to local contexts that they are implemented in. These linkages extend to how a given trust activity's accountability structures, legal certainty, data infrastructures, applications, and their relation to the local economy, local actors, and communities. (Bodó, 2021) This perspective is assured by others who posit that not only trust-building activities but also the success of enacted artifacts is a product of how well they fit the surrounding environment, and such an environment should allow for adaptations for governance and management. (Sedlmeir & Weigl, 2022) Governments are found to be market-makers in the EUDI ecosystem, and their capabilities to initiate successful governance are elemental to ecosystem success. (Degen & Teubner, 2024) To harness the strategic governance role of the government, scholars argued that governments have to have an overview of the interdependencies of the ecosystem and construct governance processes beyond technical requirements. (Degen & Teubner, 2024) In sum, we derive our motivations in tandem with the problem space and the relevant literature, which suggests practical gaps in the digital identity governance space and particular readiness challenges for Member States to execute value creation mechanisms in a complex digital platform ecosystem. The literature outlook suggests that EUDIF, as a pan-European Regulatory framework on cross-border identity, is an ecosystem with the ability to project its characteristics on institutions, affecting their trust practices, and processes. The success of its value propositions may ultimately

depend on governance dynamics and the capability of actors to harness ecosystem value creation mechanisms. In our aim to contribute to the scholarly domain within the identified knowledge gaps and to offer practical insights towards governance of novel trust and governance concepts from the EUDIF regulatory framework, we aim to inform the design of a governance model artifact based on Design Science knowledge. We aspire to position our contributions to function as an intra-organizational building block in the public sector towards achieving the full scope of public value creation using digital identity wallets. Given the considerations and scope of our problem space and motivation, we present our research goal.

RG1: How can an intra-organizational governance model be designed to inform value creation via the adoption and use of EUDIWs in public sector organizations?

2.3 Research originality, value, and contribution

Our thesis mainly contributes to the practical governance challenges of public sector organizations in the EUDIF ecosystem. We identify practical organizational, individual, and ecosystem-level constraints, barriers, drivers, and digital identity wallet adoption antecedents and propose organizational structures, controls, processes, and hierarchies via a final governance model in order to enable public sector organizations to deal with adoption complexities. By achieving this, we make original contributions to the body of knowledge on organizational-level digital identity governance and deliver auxiliary learnings to digital identity adoption research, EUDIF, and digital identity wallets research streams. Our research is the first of its kind to focus on public sector organizational governance aspects of the EUDIF, employing a design knowledge approach that incorporates perspectives from a multiplicity of ecosystem actors. We posit that our contribution is especially timely considering the concrete EUDIW adoption deadline for public sector organizations and aspirations of the technical community, private sector organizations, and Member States to accelerate digital identity wallet adoption in public sector use cases and to enable the realization of value via service delivery. Our findings can be reused by public sector organizations to customize internal-governance models or by EUDIF practitioners focusing on adoption and governance aspects of EUDIWs in the public sector.

3 Literature review

This section provides a detailed account of our literature review process. We have structured our literature review process in alignment with Webster and Watson's proposed framework on constructing literature reviews in IS domain. Within this chapter, we will aim to survey and synthesize adjacent research streams. (Webster & Watson, 2002) In our literature review, we will support our analysis with a conceptual classification model. (Webster & Watson, 2002) Of the existing adjacent research streams, we attempt to synthesize our findings to propel our research. The existing literature on the European Digital Identity Framework and the European digital identity wallets is nascent and fragmented. (Lukkien et al., 2023) This aspect presents a minor challenge to researchers who would approach a given problem from multiple actors' perspectives, as studies providing contextualization of the EUDIF or the digital identity wallets in sectoral domains are lacking. Furthermore, the current literature on digital identity wallets lacks satisfactory empirical inquiry on the topic of governance from a perspective of the number of articles published on the topic. The following sub-sections will be dedicated to establishing the necessary background for our study. We will offer a Survey of the relevant Regulatory context and introduce concepts.

3.1 Literature background

We will dedicate this section to introducing the necessary conceptual elements from the perspective of regulatory frameworks. A clear and well-defined conceptual structure is relevant to ensure our methods and results can be understood by the audience. Our analysis of the regulatory framework backdrop will be a subsection of the whole regulatory text, as we only aim to demonstrate relevant concepts for our research goals. We will only focus on presenting relevant pan-European regulatory frameworks, as reviewing national frameworks reaches beyond the scope of this thesis. Concepts will be introduced to the extent that they bear relevance to the research questions and problem statement presented in the previous chapter.

3.2 eIDAS Regulation

Regulation 910/2014, or the eIDAS Regulation, on electronic identification and trust services for electronic transactions has been the landmark regulatory initiative to define a pan-European framework govern the operation of digital trust services, establish a legal framework for electronic trust components such as electronic signatures and frame conditions the cross-border recognition of electronic identification means of natural and legal persons in the European Union. (European Commission, 2014) Within its scope, the Regulation enabled certain digital transactions to be ascribed with legal value and facilitated the use of digital identifiers for citizens to be used across union borders to carry out electronic transactions towards digital public services. (European Commission, 2014) Concepts such as 'electronic identification means', 'PID', 'relying party', 'electronic identification', and 'authentication' were defined in a pan-European context. Sequentially meaning, a unit containing person identification data to be used for authentication for an online service, a set of data enabling the identity of a person to be established, a party that relies upon electronic identification or a trust service, process of using person identification data in electronic form to represent a person and an electronic process enabling electronic identification of a person. (European Commission, 2014) Since its adoption, Member States have had the obligation to recognize and enable the use of electronic identification means recognized at national and union level, and enable their use towards authenticating with digital public services and performing electronic information processing per Article 6. (European Commission, 2014) Proposed 'assurance levels' prescribe levels of mutual trust in the operational and technical security of the notified electronic identification means and therefore access to cross-border digital public services for cross-border public service clients dependent on possessing a recognized credential with an adequate level of identity assurance accepted by a digital public service. (European Commission, 2014) Notification of electronic identity identification means by member states has not been made mandatory. (Weigl et al., 2022) Availability of electronic identity means towards cross-border public services rest on the condition that notifying Member States make a minimum number of compatible digital public services available and establish a certain degree of technical interoperability to ensure secure cross-border identity transactions. (European Commission, 2014) Limited measures were taken to include non-public sector users in the scheme (Weigl et al., 2022), and transactions were envisaged to be free of charge. (European Commission, 2014)

Liability clauses were enacted to hold Member States accountable for undesirable conduct or negligent behavior through the identification channels. (European Commission, 2014) In terms of cross-border interoperability, principles of technology agnosticism and privacy by design were steadfast, as several interoperability principles and practices were established around the use of European standards. Furthermore, multiple collaboration channels between Member States, ranging from communication security, technical standardization, and good practice information sharing, have been established. (European Commission, 2014) The Regulation also established supervisory bodies in governance roles to oversee the certification and compliance of trust service providers, which then repurposed their services to trust service subjects as natural or legal persons. (European Commission, 2014) Introduction of a pan-European trusted list ensured that cross-border transactions can be electronically verified through a trusted third party's mediation. Trusted lists include recognized trust service providers, which are essential intermediaries that provide electronic trusted artifacts, such as electronic signing and authentication certificates for the electronic backchannels of public digital service delivery. (European Commission, 2014) Use of recognized electronic signatures and similar trusted artifacts was recognized in cross-border service delivery contexts alongside electronic documents. Effectively, establishing legal grounds for cross-border mutual recognition of electronic identification means for the first time in the European Union. (European Commission, 2014; Weigl et al., 2022)

3.3 The European Digital Identity Framework Regulation (EUDIF)

Following the adoption of the eIDAS Regulation, the European Commission put forward a proposal for a European Digital Identity Framework in 2021.(Ramona, 2021) Building on top of the achievements of the eIDAS Regulation since its adoption, the proposed framework would facilitate the sharing of identity data attributes online, enabled by a digital identity wallet. (Ramona, 2021) The drive for change has undoubtedly arisen from union-level policymaking (Weigl et al., 2022) which will be relying on the establishment of secure, cross-border capable authentication of persons and companies throughout the European Union for the achievement of the Digital Decade Program where the uptake of national electronic identities are enumerated as a primary success metric (European Commission, 2022) and technical policymaking priorities around digital sovereignty, data control, competitiveness and strengthening the propositions of the Digital Single Market. (Weigl et al., 2022) Substantiating the need for the framework, the European Commission

posited that a concert of evolving users' needs around electronic identification and individual electronic identification means' adoption shortcomings (Kubach et al., 2020) related to the implementation of eIDAS Regulation (Weigl et al., 2022) has necessitated an update. Previously, the Regulation had not mandated Member States to notify electronic identification schemes; hence, adoption of notified schemes has remained stagnant under the current policy framework. (Weigl et al., 2022) Individually, European citizens' interactions with digital spaces have been transformed since the first policy formulation rounds of the eIDAS Regulation. Since the advent and uptake of very large online platforms, user digital identity transactions have been happening predominantly inside large online platforms. (Kölbel et al., 2022) At the same time, electronic identification use towards e-government services stayed considerably stagnant even in pioneering European countries. (Kubicek & Noack, 2010) However, large online platforms have not made sufficient progress towards transparency in their user-centric or federated identity management systems (Kölbel et al., 2022). Users' oversight and control over the handling and processing of their data remains limited, with heightened concerns over data monetization, trafficking, and security. (Kölbel et al., 2022) Such bottom-up concerns around personal data protection gained traction in policymaking. Adoption of the General Data Protection Regulation (GDPR) in 2018 has been made in a digital environment where personal data protection has been getting heightened concerns. (Ramona, 2021) Introduction of GDPR as a premier regulatory framework in data governance has had lasting effects in the policy ambitions of the European Union and cast its reflections for the next decade of policymaking around similar issues. (Weigl & Reysner, 2024) Since the turn of the decade, European public sector organizations have had time to innovate with digital identity in times of crisis, offering smartphone-based identity and attribute sharing solutions like digital vaccination certificates at the height of the COVID-19 pandemic.(Weigl et al., 2022) At the same time, concepts such as self-sovereign identities and verifiable credentials have achieved higher levels of maturity. As a result, more trust concepts have been made available to policymakers. (Ramona, 2021), (Weigl et al., 2022), (Weigl et al., 2023). In sum, a concert of policymaker and societal-level concerns, combined with the availability of technical solutions, gave way to an initiative for transforming the pan-European regulatory frameworks from regulating electronic identification and cross-border access towards data-use and control prerogatives (Weigl et al., 2022)

Following European-level consultation and decision-making processes, the European Digital Identity Framework (EUDIF) was adopted in 2024 and is currently going through an implementation phase within the Member States. (European Commission, 2024) EUDIF, increased its scope over eIDAS Regulation to introduce new trust concepts and a multi-actor digital ecosystem situated around the use of a digital identity wallet, for the first time the scope clearly included private sector participation: "...enable persons to exercise their right to participate in digital society safely and access online public and private services throughout the Union." (European Commission, 2024) Certified digital identity wallets are introduced as electronic identification means that are mutually recognized by Member States on top of the existing electronic identification means classifications of the earlier Regulation. Defined as an electronic identification means that allows a user to store, manage, and validate person identification data (PID) and electronic attestations of attributes (EAA) for the purpose of providing them to relying parties and other users of European digital identity wallets. (European Commission, 2024) In this definition, electronic attestation of attributes (EAA) means an attestation in electronic formats that allows an attribute of persons or objects to be authenticated; such attributes can be issued on behalf of public sector bodies responsible for an authentic source of personal attributes or by private sector actors. Public sector electronic attestations of attributes (Pub-EAA) are functionally different than other EAAs and their lifecycle is governed by special clauses in the Regulation. An authentic source is a system, under the responsibility of a public sector body or private entity, that provides attributes for persons or objects as a primary source of information in law or practice (European Commission, 2024) The European Digital Identity Wallet is conceptualized as a technical means to offering "…secure, seamless and cross-border access to public and private services while having full control over their data…" in addition, wallets are to ensure the possibility of selective disclosure of data, enable the use of pseudonyms and privacy preserving features such as unlinkability, facilitate personal data control at relying party level and enable all of such functionalities in a under-friendly, transparent and traceable manner. (European Commission, 2024). Provision of recognized digital identity wallets has been made mandatory with clear deadlines; wallets can be offered by a Member State or under the mandate of one. Alternatively, recognized independent solutions are possible. (European Commission, 2024)

Relying parties represent a big chunk of the EUDI ecosystem. Public sector relying parties, as well as a select portion of private sector actors such as very large online platforms and service providers in specific industries, currently carry the obligation to support European digital identity wallet use cases by the end of 2026. (Weigl et al., 2022) To facilitate transparency on their side, relying parties will have to be registered via designated registrars and communicate their use case with the wallets, which will form the basis of their transaction scope, communicate with the wallet through common interfaces, and support essential functionalities of the wallet. (European Commission, 2024) The Regulation introduces a requirement for Member States to allow qualified trust service providers (QTSP) issuing qualified attestations of attributes to verify a pre-defined set of attributes' authenticity via authentic source operators at national levels or by their recognized intermediaries given that such attributes rely on data supplied by authentic sources operated by the public sector. (European Commission, 2024) Overall, the trust framework is executed by a concert of artifacts, lifecycles, and a centralized registry of actor attributes, operation scopes, and entitlements, and transparent verification of such attributes by other participants via electronic certification systems. (European Commission, 2025)

The Architecture and Reference Framework (ARF) document, developed by the European Commission, aims to develop an architectural blueprint of the upcoming EUDI ecosystem. The blueprint includes specifications, guidelines, and conceptual groundwork for the implementation of the Regulation. ARF recognizes the EUDI initiative as an ecosystem where use cases, user experience, value propositions, and ecosystem requirements are recognized and documented. ARF recognizes several use cases of the ecosystem, and several of them directly relate to the delivery of digital public services, such as facilitating access to government or private sector data or authentication to digital service channels via the reuse of personal data. (European Commission, 2025) Most importantly, ARF extensively describes EUDI ecosystem roles and relationships.

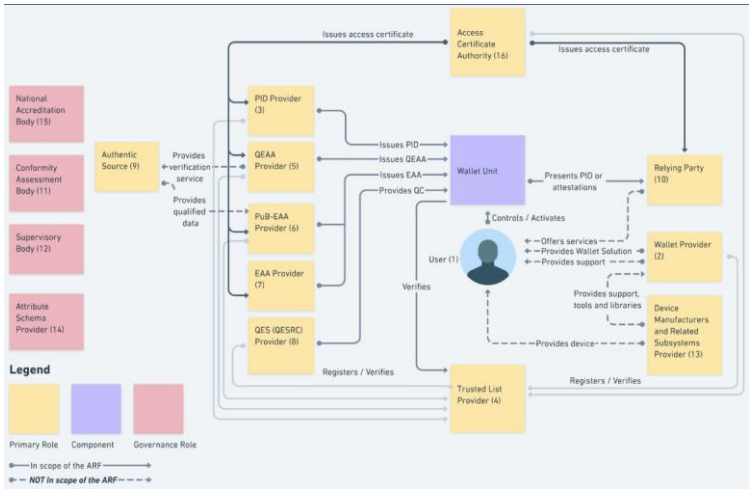

Figure 1 Ecosystem roles in Architecture and Reference Framework (ARF) From (European Commission, 2025)

In summary, a large part of the ecosystem consists of wallet users, providers of EAAs (as both (Q)EEAs and Pub-EAAs), PID, authentic sources, relying parties, and wallet providers. Activity constraints exist for wallet providers, data providers, and relying parties who are to be registered in pan-European trusted lists or with relying party registrars. Based on a cross-reference of requirements between the ecosystem map and the EUDIF Regulation, we can ascertain that a wallet provider can be a government entity or a private entity recognized by a Member State. Authentic sources can be operated by a public sector entity or a private entity on behalf of a public sector entity, users can be natural or legal persons and data providers to the wallet (EAA, PID, (Q)EAA and Pub-EAA) can be private or public entities as trust service providers who meet the requirements enumerated in the Regulation and related technical specifications to be certified into their role. Relying parties can be public or private entities that meet the requirements to be recognized as a wallet relying party or utilize ‘intermediary’ relying parties to fulfill their obligations towards the wallet. Intermediaries are recognized as a special class of relying parties with an additional set of requirements for operation.

The ecosystem incorporates several core design principles, attached to its goals and aspirations for the future of the mediated digital trust infrastructure in the European Union. We consider these core and supporting design principles, as well as overarching ecosystem goals, vital inputs for contextualizing our artifact generation process. In order to take stock of such principles and goals exhaustively, we generated a table of enumerated points as presented in the Architecture and Reference Framework. (European

Commission, 2025) This table has been provided in the appendix of this thesis, accessible in the Annex O

3.4 Literature review concept matrix

In this subsection, we demonstrate our literature review concept matrix. (Webster & Watson, 2002) We generated a concept matrix of the immediate research domain of digital identity wallets, as the research domain lacks substantial empirical volume., With a total of 10 directly related articles identified, we employed a broader conceptual perspective and identified all conceptual linkages presented in the articles. Our literature review will follow with discussions of identified concepts presented in the concept matrix. The resulting concept matrix has been attached to the appendix of this thesis, accessible in Annex B.

3.5 Contextualizing Digital Identity Wallets in the Public Governance domain

In this section, we will offer a contextualization of the digital identity wallets in the public governance research domain. Without a doubt, the vanguard initiative of the European Digital Identity Framework (EUDIF) has been the digital identity wallet ecosystems with wallet artifacts at the core, surrounded by types of data elements with adjacent data sharing and trust infrastructures. (European Commission, 2024) The wallet technology, since its inception from a policy perspective, has gotten increasing amounts of attention from various stakeholders. However, wallets are conceptualized as primarily technical artifacts in early literature (Podgorelec et al., 2022) and touted for their technical capabilities. As a result, they have been relevant to the information systems domain because of their technical characteristics and abilities. The adoption of EUDIF has ascribed this concept multiple new dimensions that are closely linked to the public governance domain. Firstly, the Regulation recognizes wallets with adjectives such as ‘privacy preserving’, ‘enables full control over one’s data’, ‘transparent’, ‘means to exercise data portability rights’, and ‘user-friendly’. (European Commission, 2024) Moreover, the renewed Regulation focuses on the individual as a public service client as the driving actor in identity-related activities. (Weigl & Reysner, 2024) Subsequently, the digital identity wallets in the European context have not only been mere technical artifacts but evolving socio-technical systems with a certain degree of expectancy that development, use and adoption of such may enable specific public values such as

transparency and data controllability (Marsman et al., 2024) Notwithstanding with the regulatory developments, contextualized synthesis on digital identity wallets have been lacking in information systems and public governance research streams.

Governance of digital identity initiatives has been identified as a 'wicked problem' (Weigl & Reysner, 2024) Scholars attribute 'wickedness' to regulatory aims to tackle interest balancing initiatives between public sector, private parties, and individuals in an ecosystem where simultaneously aiming to tackle "… institutional trust, autonomy and control as well as privacy, oversight and accountability at the same time…" (Weigl & Reysner, 2024) it is also found to be ubiquitous in our day and age (Weigl & Reysner, 2024) and high risk, owing to the amount of sensitive data and trust pouring into the ecosystem. (Weigl & Reysner, 2024)

The EUDIF framework aims to be technology-neutral. (European Commission, 2025) and thus does not propose linkages between regulatory concepts and existing technologies. This aspect introduces challenges for researchers to establish linkages between existing technological artifacts, such as Self Sovereign Identities (SSI), that may exhibit considerable similarities to the European Digital Identity Wallets in terms of their conceptualization, technical capabilities, and design considerations. However, research on this very issue remains limited. However, researchers posited that European Digital Identity Wallets may be a subset of Self-Sovereign Identities (SSI), (Degen & Teubner, 2024; Weigl & Reysner, 2024) Thus, enabling us to proceed with the inclusion of Self-Sovereign Identities in our review process.

Our overview of the EUDIF regulatory framework in the previous chapter clarified recognized actor roles, expected behavioral dynamics of collaboration, and co-production of digital value. However, the regulatory framework, comprised of the renewed eIDAS Regulation and the Architecture and Reference Framework (ARF), does not attempt to clarify interactions and relationships between recognized actors. This has resulted in contextualization gaps in our thesis as we attempt to position the EUDI initiative in relevant streams of literature. We suggest that, based on our elaboration of the research background, the EUDI initiative exhibits fundamental characteristics of digital ecosystems from multiple angles. We attempt to bridge existing conceptual frameworks and recognized entities in the regulatory framework for enhanced conceptual saturation of our literature review going forward. To this end, we suggest that the multi-actor EUDI

ecosystem falls under the definition of an ‘innovation ecosystem’ (Granstrand & Holgersson, 2020), a ‘digital public platform ecosystem’ (Hein et al., 2020) and a ‘public service platform’ (Bender & Heine, 2021), and the EUDIW is a ‘public service delivery means’ (European Commission, 2024) and a ‘multi-sided platform’ (Hagiu & Wright, 2015) EUDI ecosystem enables the collaboration of different role entities for credential based data sharing. The cornerstone component of digital identity wallets is building blocks for innovative parties to offer their service and product innovations to citizen-users, businesses, and public sector organizations. Furthermore, the EUDI ecosystem exhibits traits of a digital identity ecosystem. Scholars posit that conceptually, a digital identity ecosystem comprises (1) an ecosystem concept with a purpose, context, and key definitions. (2) technological and governance blueprint definitions with technical architecture, defined technical components, governance rules and policies, as well as interoperability considerations. (3) business models that incorporate revenue models, considerations around costs, risks, and process changes. (4) Collaboration models that take into account the role of orchestration, adoption, and ecosystem processes. (Kolehmainen, 2021)

3.6 Adoption of digital identities in the public sector context

In this section, we present the positions from the literature on organizational adoption of digital identities in the public sector. Value creation in a dynamic ecosystem by a public sector entity necessitates a degree of adoption of ecosystem components by institutions and public service clients. In this case, the adoption of digital identity wallets by public service clients and public service co-enablers, such as businesses, is a crucial first step for ecosystem development. (Bochnia et al., 2024) Adoption of digital identities can be understood from a user or institutional perspective. We utilize the broader digital identities research domain to derive relevant insights on both actor perspectives. Researchers suggest that the antecedents of self-sovereign identity adoption are a collection of environmental factors, including country, cultural, industry, organizational, civil society, and individual positions, behaviours, and attitudes around the technology. (Kolehmainen, 2021; Laatikainen et al., 2025) Thus, reviewed articles incorporating individual, group, and organizational levels of adoption analysis.

3.6.1 Challenges of institutional adoption of digital identities

Empirical investigation of institutional adoption challenges reveals that public sector organizations' adoption can be challenged by citizens' perception of the difficulty of eID system use. (Liesbrock & Sneiders, 2024) Institutional preference for alternative methods of identification can be elicited as a result of poor citizen adoption. (Liesbrock & Sneiders, 2024) Institutional perception of poor adoption of digital identities by individuals can result in inaction from institutions. (Liesbrock & Sneiders, 2024) Lack of well-defined use cases of electronic identities affects institutional and individual adoption motivations negatively. (Liesbrock & Sneiders, 2024) Use case related challenges can render a digital identity solution towards infrequent use, which can elicit low motivation towards keeping the project ongoing and drive perception of low benefits attached to institutional adoption of digital identities. (Liesbrock & Sneiders, 2024)Moreover, a lack of awareness about digital identity system success and an unclear fit of digital identities on top of existing service offerings have been identified as additional challenges. (Liesbrock & Sneiders, 2024) Another challenge dimension is that organizations can perceive the necessary digital transformation as infeasible or may lack the resources. (Liesbrock & Sneiders, 2024) Adoption challenges can also be underpinned by a mismatch between institutional digital identity requirements and capabilities offered by technical solutions. SSI use may introduce legal uncertainties in business processes, immaturity of technical specifications, as well as a lack of documented best practices, which can introduce use constraints. (Bochnia et al., 2024) Immaturity challenges can be exacerbated by users' unwillingness to pay for identity solutions early on. However, it has been suggested that the development of network effects can stimulate paid business model development. (Kubach & Sellung, 2021) Further research enumerates management attitudes, organizational culture, organizational financial condition, access to resources, innovativeness, age and size of organizations, technological competences, and awareness of regulatory compliance activities, as well as awareness around privacy and security, along with incentive structures, are determinant conditions for adoption. (Kolehmainen, 2021; Laatikainen et al., 2025)

3.6.2 Challenges of individual adoption of digital identities.

Empirical studies exist to scrutinize digital identity wallet adoption challenges from an individual perspective. Scholars suggest that individual skills and competencies, attitudes

about using digital identities, individual agency, sensitivity towards relevant challenges around digital identity use, and subscription to human-centric principles, as well as access to proper resources, are enabling conditions for digital identity adoption for individuals. (Laatikainen et al., 2025) It has been suggested that the adoption of self-sovereign identities can be challenged by existing forms of identification based on convenience and availability. (Korir et al., 2022) Over-sharing of identity data to relying parties has been found to be a salient concern for individuals. (Korir et al., 2022) Users have been found to derive trust from existing legal conditions around data protection and control over identity data sharing in such instances. (Korir et al., 2022) Individual perceptions of service level details, such as processing times and convenience, are yet another determinant for adoption. (Korir et al., 2022) It has been emphasized that relying party data control hierarchies are important considerations to individual adopters, such as the scope of the relying parties' asking for identity data, and that there might be uncertainty over who controls their identity data. (Korir et al., 2022) On the same topic, adopters can express disapproval of inter-organizational sharing of their identity attributes between relying parties. (Korir et al., 2022) Individual adopters might assign trustworthiness levels to relying parties, leading to heightened concerns about data oversharing as well as adoption or non-adoption behaviour of digital identity solutions on a case-by-case basis. (Korir et al., 2022) Individual mental models of identity data sharing behaviour, such as over-asking or under-asking in certain conditions, can be in mismatch with relying party asking behaviours, leading to distrust or confusion. (Korir et al., 2022) Privacy preserving features of the wallet such as pseudonym generation are found to be not always self-evident to users, (Lockwood, 2021) primarily when optionality of sharing an attribute is not defined in a relying party process; data minimisation might have to exist in a supporting environment where processes allow for minimisation rather than merely suggesting it. (Korir et al., 2022) Individuals might question the efficiency of the attribute presentation processes towards a relying party, questioning the value of the wallet as an enabler versus an additional burden imposed by a decentralized inferior alternative (Lockwood, 2021), as relying party processes might be ever so slightly different. (Korir et al., 2022) Furthermore, components of the wallet might not always be intuitive for users, suggesting learning curves and hurdles with onboarding and operating the wallet. (Korir et al., 2022), Moreover, social exclusion, increased responsibility for owners and operators due to decentralization, and, as a result of relinquishing organizational data custody, are explored themes in research. (Lockwood, 2021)

3.6.3 Environmental and ecosystem factors for digital identity adoption

Often, digital identities are not standalone products or artifacts but wrapped in environmental and ecosystem constraints and conditions that affect adoption outcomes. Scholars suggest that country characteristics such as regulation and legislation dimensions, governmental attitudes around technology, processes, and hierarchies in the public sector, trust in government, and social norms affect the preconditions of adoption. (Laatikainen et al., 2025) Furthermore, industries can shape precedents of adoption by setting the playing field around the level of digitalization in the industry, industry regulations and standards, and defining the need for verifiable data. (Laatikainen et al., 2025) Characteristics of technologies also play a role in determining the level of compatibility, complexity, user experience, interoperability, and maturity of the available solutions. Conversely, such technological outcomes interface with ecosystem conditions to set relative advantages, security, and privacy concerns of adopters. (Laatikainen et al., 2025) Ecosystem conditions set the monetary or non-monetary incentives, business, technical, and legal policies, and principles that may have a direct impact on adoption. Ecosystem actors' credibility may also carry implications for adoption. (Laatikainen et al., 2025) While uncertainty, lack of harmonized regulations and standards, and information asymmetry in ecosystem conditions can negatively affect adoption (Kolehmainen, 2021) In this case, expert communities and non-profits can play an active role as access and engagement channels. (Kolehmainen, 2021)

3.6.4 Drivers for digital identity adoption

Considering the multi-faceted nature of digital identity adoption, scholars have found adoption predictors on multiple levels of analysis, organizations might be motivated to garner conditions for increased security, cyber-risk reduction, customer satisfaction, brand value improvements, learning and innovation opportunities, increased performance and competitive advantage generation, increased regulatory compliance and resource and process efficiency as well as cost savings. (Laatikainen et al., 2025) Furthermore, organizations might find benefits in the digital sovereignty dimension, offloading of data stewardship responsibilities, availability of high-quality data, and increased trust in customer relationships, especially for Know Your Customer (KYC) processes. (Lockwood, 2021) Environmentally, ambitions towards adoption outcomes might come in the form of expectation for more trustworthy, private and secure digital interactions,

giving citizens more data control and privacy and decoupling digital identities from centralization (Lockwood, 2021), generating more opportunities for social equity, democratization and liberties (Kolehmainen, 2021; Lockwood, 2021) and more efficient public service delivery. (Lockwood, 2021) increased job performance, digital inclusion, and achievement of digital transformation goals. However, considerations have to be extended towards possible misuse of such systems. (Laatikainen et al., 2025) From an ecosystem perspective, the generation of economic advantages, the creation of strategic alliances, increased collaborative performance, and the discovery of new markets, structures, and businesses are enumerated as predictor motivations for adoption. (Laatikainen et al., 2025) Individual adoption can predict increased job performance, building of skills and competencies, increased self-esteem, and generation of individual trust. (Kolehmainen, 2021)

3.7 Public digital identity ecosystem governance

Across disciplinary boundaries, scholars have observed linkages between the EUDI Wallet initiative and government-orchestrated digital public infrastructures. (Degen & Teubner, 2024) The Regulation, by virtue of striving for the inclusion of public and private organizations (European Commission, 2024), has created not only multiple stakeholder roles but also a government orchestration role where responsible Member State organs will bear the task for unlocking value creation in a complex data ecosystem. (Degen & Teubner, 2024) By undertaking such a role, Member States will have to enact strategic and dynamic processes to manage and coordinate ecosystem participation through the exploitation of digital public infrastructure and government data to stimulate the generation of collaborative value, trust, legitimacy, accountability, and efficiency in the ecosystem. (Degen & Teubner, 2024) Authentic government data is seen as a business driver by private sector entities as data reuse can unlock procedural simplification (Kubach et al., 2020) However, a large subset of government data exists in non-SSI friendly formats such as digitized copies of paper attributes. In centralized registers, management of such data introduces technical, monetary and organizational costs to data custodian organizations. Currently, such data is managed in a push principle, meaning that custodians push updates and maintenance controls onto data artifacts. (Kölbel et al., 2022) Subsequently, government data reuse has been underlined as an important participation incentive for the whole ecosystem. Reuse initiatives might ease data management burdens of the orchestrator if such data artifacts were open to trusted reuse

practices, effectively enabling organizations with verifier roles to build business models around verification and issuance of said data to wallets and relying parties, this approach might not only incentivize public sector data sharing but also increase quality of authentic data in circulation through persistent verification and circulation mechanisms. (Kölbel et al., 2022) From this lens, allowing widespread secure sharing of authentic data is seen as an enabler to potentially weaken intermediary use cases, as such business models thrive on higher transaction costs on data sharing, as well as ensuring data portability capabilities. (Kölbel et al., 2022) Enabling data sovereignty in organizational processes might introduce operational challenges to data sharing use cases as users are empowered by digital identity wallets to selectively disclose identity attributes, perform transactions pseudonymously, and exercise data portability, meaning that user data can be taken out of organizational data processing contexts meaningfully. (Kölbel et al., 2022) Such cases might introduce breaking changes to existing business processes for public sector organizations.

Scholars not only explored the general dynamics of digital platform ecosystems but also the emerging ecosystem of EUDIF. The primary responsibility of Member States is to execute governance mechanisms to unlock value creation, manage tensions, and create value through collaboration. (Degen & Teubner, 2024) Degen & Teubner iterate that this ecosystem "..comprises issuers of identity data, ID wallet providers, relying parties, users, the orchestrator/regulator, and the ecosystem service providers.." This ecosystem's performance is underlined by inter-entity data sharing abilities and practices. (Degen & Teubner, 2024) Orchestrator's principal actions play an important role in creating incentives and reducing technical, socio-technical, economic, and regulatory barriers to participation and value creation. (Degen & Teubner, 2024; Kubach et al., 2020; Weigl et al., 2023) Another dimension of the orchestrator role is to balance standardization, technical requirements, certifications, technical artifacts' use cases, and interoperability levels necessary for ecosystem participation. (Degen & Teubner, 2024; Sedlmeir & Weigl, 2022) However, ensuring common interoperability and standardization levels is challenging as it requires alignment of various trust levels and frameworks, ecosystem IT structures, enactment of semantic interoperability between trusted peers and regulatory consistency (Degen & Teubner, 2024; S. Lips et al., 2020) To ensure increased ecosystem participation incentives, harmonization of trusted artifacts' user experience (UX), entry requirements for new ecosystem players in the form of high investment costs and data

issuers' concerns over data use and generation might need to be addressed. (Degen & Teubner, 2024) While it is expected that the EUDIF ecosystem will generate new business models, incumbent business models in Member States may offer resistance to new entrants. (Degen & Teubner, 2024) Relying parties constitute a large base of organizations expected to be active in the ecosystem. Relying parties can be private sector organizations, public sector, and even individual users. It has been asserted that relying parties may prefer systems that generate less friction for onboarding; these solutions may ideally be balancing cost and security at an equilibrium. (Kubach et al., 2020) Crucially, orchestrators need to demonstrate the ability to perform their role and possess the capabilities to generate specific ecosystem outcomes. (Degen & Teubner, 2024) Awareness communication from the orchestrator towards other participants is valuable to bolster incentives for participation. (Degen & Teubner, 2024) Furthermore, orchestrators can utilize their unique position to offer trust building activities to participants by incorporating their outputs as inputs to activities under orchestrator purview (Degen & Teubner, 2024) While mandatory use of digital identity wallets can help an ecosystem attain crucial adoption rates in infancy stages, its value creation potential can be unlocked by popular client demand, existence of complimentary ecosystem services, competition and regulatory pressures. (Degen & Teubner, 2024; Kubach et al., 2020; Weigl et al., 2023) Furthermore, the Value of government orchestrators as the primary trust-building actors in the ecosystem has been emphasized. (Degen & Teubner, 2024; Giannopoulou, 2023b) On the issue of centralization and decentralization tensions in the ecosystem, it is important to recognize the responsibility of existing centralized organizations for maintaining digital public infrastructures (Giannopoulou, 2023b).

Tensions may exist between the uniformity of designed components and their variety, security, and privacy dimensions of solutions. (Degen & Teubner, 2024) From an integration perspective, clear standardization, the existence of integration support services, and subsequent reduction of technical and organizational complexities have been found essential. Transparent and straightforward solutions may attain critical network effects by integrating a number of services and functionalities that users and other relying parties find increasingly relevant, effectively harnessing a lead position. (Degen & Teubner, 2024) As with many other ecosystems, data portability and interoperability of solutions may hinder users' choice of wallets, a challenge that can be addressed by the implementation of interoperable standards. (Degen & Teubner, 2024)

Balancing of concerns between security and privacy can lead to considerations on the choice of technical solutions, such as the choice between utilizing centralized or decentralized solutions for data processing. (Degen & Teubner, 2024) Nonetheless, such balancing concerns might be trumped by the existing digital identification practices and defaults of the playing field, rendering blank-slate ideal approaches not ideal for some use cases. (Degen & Teubner, 2024) The business model of a wallet provider might ultimately rely on more complex transactions, including multiple data attributes in aggregation via different sources, including different relying parties, to create economic incentives for participation. The lack of well-defined use cases may act as entry barriers, as a data-poor ecosystem in that aspect would introduce more hindrances for co-producers of a service component. (Degen & Teubner, 2024) Ultimately, users' expectations of ecosystem services might determine what type of services become prevalent. (Kubach et al., 2020) Considering the public-private partnership tensions, co-producers of public digital services might not always share a set of motivators unequivocally. Profit motive and public value creation can be exhibited by collaborating parties in a conflicting context. (Whitley & Schoemaker, 2022) Attribute providers might be hesitant to comply with ecosystem entry requirements as they are unaware of other participants' intentions and awareness towards utilizing their solutions, especially since the regulatory framework may restrict such visibility for compliance and data protection reasons. (Degen & Teubner, 2024) Conversely, orchestrators may have the responsibility to bridge service providers to service provider business relationships as well as service providers to relying party relationships in the form of use case matching, strategic communication and awareness campaigns, and transparency controls. (Kölbel et al., 2022) Orchestrators might have to balance participation frequencies between distinct ecosystem participants to balance the distribution of access and power. Clear delineation between ecosystem roles has been suggested as a factor to help orchestrators balance ecosystem participation. (Kölbel et al., 2022)

From the lens of individual ecosystem participants, particularly governmental organizations and private companies, EUDIF ecosystem participation is closely tied to the existence of wallet business models. (Kölbel et al., 2022) In this context, business models denote the pathways for value creation, monetization, and offering of products and services for ecosystem participants. (Kölbel et al., 2022) Considering the interdependence of actors in each identity data ecosystem, it has been suggested that

actors harness strategic bilateral partnerships, cross-sectoral collaboration, and a cooperative structure as a method of digital service delivery. (Kölbel et al., 2022) Collaboration structures can help align inter-organizational incentives and accelerate service delivery mechanisms as players engage in co-delivery of digital services with interconnected components. (Kölbel et al., 2022) A departure from value-extractive business models of identity management may mean that SSI principles of data sovereignty and privacy may be better respected; however, this may also necessitate the discovery of new revenue streams for providers of trusted data and identity wallets, whom the orchestrator will incentivize to respect SSI-based principles of data sharing. (Kölbel et al., 2022)

3.8 Self-Sovereign Identities in the Public Sector

In this section, we will consult the Self-Sovereign Identities research domain, as they are the umbrella term under which the EUDIWs are situated as a specialization of. Self-Sovereign Identities have been around in the academic domain significantly longer than EUDIWs. Garnering scholarly attention as early as the 2000s. (Ferdous et al., 2019) On the topic of Self-Sovereign Identities (SSI), scholarly emphasis on the recent development of the concept has been focusing on it being a value-laden concept, as it has been found to be used in conjunction with models and concepts related to decentralization. (Weigl et al., 2023) Furthermore, SSIs have been vaguely defined in theory and practice (Giannopoulou (Alexandra) & Wang (Fennie), 2021) What an SSI might look like in real world may relate to underlying policy goals associated with a given project, so much so that conceptual vagueness may be interpreted in different directions by stakeholders. (Weigl et al., 2023) Ambiguities from technological and socio-political lenses of the concept have introduced challenges from an implementation standpoint in the public sector. (Cheesman, 2022; Weigl et al., 2023) Although technical ambiguities exist, SSIs are often accompanied by decentralized communication protocols (DIDs), Verifiable Credentials (VCs), which are cryptographic components that can be used as identity attribute assertions. (Weigl et al., 2023) In real-world applications, SSI ecosystems may mandate the use of a digital identity wallet, interlocking two concepts together. (Weigl et al., 2023) Implementation of wallets can depend on centralized or decentralized types of data storage, offering a choice between traditional PKI implementations versus decentralized protocols for data sharing. Scholars suggest that perceptions of SSIs from government officials may include “...duty of care over users institutional prerogative over

identity matters, legal, compliance, and policy realism" (Weigl et al., 2023) SSIs may also carry public innovation undertones of data control, digital literacy, trust and credibility and decentralization while enumerated principles of SSIs might include user-centricity and privacy. (Weigl et al., 2023) SSIs may introduce conflicting interests in public sector adoption, while the public sector might ultimately value a prerogative custody transfer of citizens' data; they might see the transfer as potentially risky for organizational liability or would like to position SSIs as an intermediary artifact to garner more trust in centralization. (Giannopoulou (Alexandra) & Wang (Fennie), 2021; Weigl et al., 2023) This becomes a salient issue concerning principal ecosystem actors' accountability to ensure that other actors' identities can be established to enable accountability over transactions that happen inside the ecosystem and account lifecycles. (Kubach et al., 2020) which has been a reported but unsolved technical challenge. (Giannopoulou (Alexandra) & Wang (Fennie), 2021) Researchers have also posited that such technologies' adoption may ultimately depend on the convenience afforded to users. (Degen & Teubner, 2024; Weigl et al., 2023) Contextually, the topic of convenience carries a unipolar interpretation of positive user experience and positive use-cases to create adoption incentives. (Sedlmeir & Weigl, 2022) SSIs should be designed to elicit user empowerment, positive end-user experience, delivery of trust intermediation, efficient performance, user friendliness, and availability. (Sedlmeir & Weigl, 2022) This theme circles back to pre-identified ecosystem tensions where security and convenience (Weigl et al., 2023), as well as the maturity of use cases, might serve as negative or positive incentives for participation. (Degen & Teubner, 2024; Weigl et al., 2023) Value proposition and underlying mechanisms of SSI should be exposed to adopters to ease adoption challenges.(Lockwood, 2021) The convenience of SSI solutions might also mean that, ultimately, some centralizing elements might have to be introduced baked in to prop up the convenience value to the users, Such features may offer credential recovery, secrets management, or other high value operations while potentially introducing dependency on centralized artifacts. (Kubach et al., 2020; Sedlmeir & Weigl, 2022) Furthermore, SSIs can come with digital inclusion challenges, previously reported on their increased digital literacy requirements for users and relying parties.(Weigl et al., 2023) Barriers also exist in access to information technologies, as their use requires more technically advanced devices. (Degen & Teubner, 2024) From an implementation perspective, SSIs have been a rapidly evolving concept, carrying legal value since the early 2020s in the European Union. Scholars posit the challenge exerted on public sector

organizations to cope with rapid evolution and the complex nature of the concept, also pertaining to its newfound legal value, and their concerns on how its use relates to their prerogatives. (Weigl et al., 2023) Related to the concept of trust is the credibility dimension; credibility should be afforded to all main actors in the ecosystem, identity claims in the form of attestations should be verifiable and revocable to bolster the transparency of claims in the ecosystem. (Sedlmeir & Weigl, 2022) Ensuring the adoption of verifiable credentials as a trustworthy, mature, and transparent artifact can establish the basis for more value creation, given that actor concerns are actively being addressed. (Degen & Teubner, 2024; Sedlmeir & Weigl, 2022) Another component is the cost to acquire and operate an SSI-based solution. These costs must not be high enough to present entry barriers (Degen & Teubner, 2024; Ferdous et al., 2019; Sedlmeir & Weigl, 2022).. Scholars have also paid attention to the implementation perspectives of SSIs. Asserting that implementations may require the utilization of technology that attempts to maintain privacy, data protection, and security of identification and information transfer operations. (Giannopoulou, 2023b) However, the use of SSIs alone does not eliminate the incentives for over-asking and maintaining the status quo of non-transparent information flows in the public sector. As more self-sovereign identity-based ecosystem flourish, establishment of Self Sovereign Identity governance frameworks have become a relevant are of inquiry for implementors, they are defined as a "set of business, legal technical definitions, policies and specifications and contracts by which the members of the trust community agree to be governed in order to achieve their desired objectives." (Foundation, 2021) Self-Sovereign Identity governance frameworks may carry conceptual similarities to security and IT governance frameworks from the dimensions of guideline setting and control implementation, as well as clarifying decisions, rights, and accountabilities to encourage desirable behavior.(Sroor et al., 2022) Such frameworks should be simple for all stakeholders to understand with clear explanations of terminology and principles, they should deliver value by stating expected outcomes of rules and policies while considering essential principles, and they should be auditable while enabling their outcomes to carry authority and consideration for their scope. (Sroor et al., 2022) Researchers have discussed the relevance of modeling to empower Self-Sovereign Identity governance. Affirming that self-sovereign identity governance frameworks are an unaddressed gap in building self-sovereign identity-based ecosystems. Such frameworks will need to consider user needs, technical standards, laws, and business requirements present in an ecosystem, as well as diversity, and the dynamic and

distributed nature of stakeholders in the ecosystem. (Sroor et al., 2022) A relevant meta-model for building such frameworks is the Ecosystem Governance Compass (Sroor et al., 2022), which consists of four layers: governance to identify ecosystem actors and their roles, rights, responsibilities, and incentives as participants. The business layer identifies revenue models and costs for each role as a collection of value streams. A legal and regulatory layer identifies compliance requirements such as laws, regulations, legal standards, and technical standards, while considering agreements and contracts between actors. The final technology layer identifies technical components such as technical infrastructure, services, architecture, application components, and data artifacts. (Sroor et al., 2022) Use of self-sovereign identity governance models has been found to enable harmonization of different viewpoints through modelling capabilities, enable stakeholders to have an overview of diverse stakeholder perspectives, enable structured, systematic, and visual representation of ecosystem relationships to support visibility and discoverability of ecosystem relationships, dependencies, and value mechanisms by different stakeholders. Furthermore, modelling increased the visibility over relationships forming for new and existing stakeholders since bi-directional objectives and incentives were able to be mapped. (Sroor et al., 2022)

3.9 Governance of public digital identity systems

In the European context, there is a ubiquity of national and cross-border digital identity systems. The EUDIF sits at the intersection of European national and cross-border digital identity systems and digital ecosystems, essentially bridging standalone systems to an ecosystem setting with the introduction of EUDIWs. Researchers suggest governance implications of such systems are consequential to their success. (S. Lips et al., 2020) Owing to the conceptual linkages of the European Digital Identity Wallet as an ecosystem, we observe a suggested governance structure to "... define statuses, rules of procedure, and other contracts that describe the rights and obligations of actors involved." (Kölbel et al., 2022) Proposing that organizational structures be established to govern ecosystem value mechanisms around shared technical infrastructure and a partner ecosystem. Scholars argue for the creation of specialized boards for the governance of intra-organizational and ecosystem relationships. (Kölbel et al., 2022) While management boards can define strategy and a shared vision, supervisory activities and technical committees can help to ensure rules and regulations for ecosystem participation as well as interoperability and technical aspects of governance. (Kölbel et al., 2022) Furthermore,

forming ad-hoc specialized committees can be helpful to ensure networks can maintain good standing in the face of outside regulatory pressures and respond with compliance and resilience. (Kölbel et al., 2022) Overall, the success of these structures may depend on their ability to facilitate coordination between committees, boards, and working groups (Sedlmeir & Weigl, 2022) while maintaining a "..trustworthy and non-monopolistic.." stance on governance. (Kölbel et al., 2022)

Literature identifies multiple implementation challenges of cross-border digital public identity systems as services. Responsibilities and collaboration levels between orchestrators of digital public services delineate such challenges. (S. Lips et al., 2020) Technical interoperability challenges between orchestrating systems may arise due to conceptual inconsistencies between the needs of the ecosystem and the design of the regulatory framework. (S. Lips et al., 2020) Differences in legal interpretations of regulatory frameworks, application of national law to cross-border service design, and differing implementation practices between member states can result in service delivery fragmentation. (S. Lips et al., 2020) Organizations have reported a lack of common architectures to identify users, compliance concerns in a fast-moving regulatory environment, which can be addressed with the development of standardized test environments and improved and commodified identifier architectures. (S. Lips et al., 2020) From an individual perspective, identified challenges are end-user facing design inconsistencies, varying levels of service accessibility to the end user, and practical differences in service delivery, as well as a lack of operational support for end-users. (S. Lips et al., 2020), (Weigl et al., 2023) Proposed mitigations for individual-level concerns are clear standardization, best practice sharing, guideline development, and support services for users. (S. Lips et al., 2020)

3.10 Adoption of digital identity technologies in the public sector

Considering the focus of our study, it is imperative to survey the adoption dynamics of digital identity and identification technology adoption in the public sector. The literature availability on this topic has been nascent, with its primary focus on blockchain and Self-Sovereign Identity adoption instead of EUDIWs. Nonetheless, scholars present relevant adoption dynamics for our case. For example, the motivations of public sector

organizations to adopt digital identification technologies can be driven by the expectation of efficiency gains, the ability to harness new technologies to promote stakeholder relationships on an organizational level. (Mahula et al., 2024) On a managerial level, Mahula et. al., identifies perceived social or business value tied to technology adoption, perception of service quality improvement, specifically the existence of supporting use cases tied to the technology as a driver of public value can bolster managerial support for adoption as client's adoption of enacted technology can strengthen use cases. Managerial attitudes on (Mahula et al., 2024) Similarly, on the decision-maker level, the existence of clear use cases, availability of organizational resources, such as funding, staff availability, and expertise, as well as adequate project runtimes, have been identified as adoption enablers, and their availability throughout project lifecycles is important. (Mahula et al., 2024) Furthermore, effective project management, including stakeholder communication and feedback loops, is identified as a co-enabler. Diverse needs of stakeholder groups might be controlled by accommodating user needs, increasing usability, especially by employing familiar design patterns, and increasing user friendliness might address adoption challenges of clients. (Mahula et al., 2024)

3.11 Value creation in public ecosystems

Considering the value creation dimension of our research goal, we dedicate this sub-section to surveying value creation mechanisms and models in public ecosystems. The EUDI ecosystem comprises actors issuing, requesting, and reusing personal identification data and other authentic data attributes to enable the creation of new products and service offerings in business and public contexts. (European Commission, 2025) The reuse of data is of paramount importance. Ecosystems where data enables joint value creation are coined as data ecosystems (Ammann & Hess, 2025). Applications of data ecosystems are underpinned by more data availability, an increase in data quality, and an increase in innovation. (de Mildt et al., 2025) However, the EUDI ecosystem is distinctly different in that it is a user-centric, decentralized, participatory, and highly regulated data ecosystem where strict governance rules define collaborative data sharing and data exploitation. (European Commission, 2025) As such, it is a similar construct to a data ecosystem in application domain scope, where an open ecosystem, application-dependent data access, and privacy protection can be noted as the initiating goal. (de Mildt et al., 2025) Nevertheless, understanding value creation mechanisms in the data ecosystem will enable us to position our contributions accurately. Data is distributed in such ecosystems

with the help of technical intermediaries, which connect data sharing activities between providers and relying parties of data. The activity of sharing and the use of the intermediary are scoped by shared governance frameworks. (Ammann & Hess, 2025) As the central enabler of value in such an ecosystem, data is captured, interpreted, transformed, and exploited for value-creating activities such as services and business processes. Subsequently, data is subjected to value capture cycles that contribute to the revenue and cost structures of an organisation. Organizations can capture indirect value from data to increase the efficiency of business processes such as decision-making and optimization. (Ammann & Hess, 2025) Furthermore, actors can link organizational resources together to harness value capture and value creation from data; this aspect can enable the pooling of resources to create collaborative value from data and enable distributed business models. Such business models can look like bartering, selling, or exchanging data between ecosystem participants. (Ammann & Hess, 2025) Scholars suggest that the composition of participants, dynamics of a given ecosystem and relevant industries, distribution of critical resources between data exchanging peers, activities, foundations, and challenges to value creation and capture can determine how business models are constructed. Moreover, the design of the technical and governance intermediaries can underpin participation costs, the nature of value capture activities, and value distribution between exchanging peers. (Ammann & Hess, 2025) An empirical study on the typology distribution of data ecosystems suggests that application-constrained ecosystem environments, like the EUDIF where EUDIWs are the primary applications. Those types of ecosystems may primarily enable the building of complementary services along service business models, governance tools, matchmaking, standardization, software as a service, consultancy, and auditing. (de Mildt et al., 2025) Configurations of data ecosystems contribute to their success. It has been found that the existence of technical boundary resources, domain specialization, architecture centralization, and the number of actors in an ecosystem are the most salient factors for configurational success. (Kernstock et al., 2025) Similar observations have been recorded specifically for the configuration of the EUDIF ecosystem as well (Lukkien et al., 2023).

3.12 Orchestration of governance in public digital ecosystems

As explored previously, the ecosystem success of the EUDIF may be underpinned by the success of the orchestration functions. Ecosystems are remarkably different than chain-based methods of value co-production. (Autio, 2022) The existence of multiple competent

actors dissolves the reliance on steered co-production of value. Hence, public digital ecosystems rely on strategic governance of participant inputs to deliver participatory value creation; such participation is often voluntary, and actor persuasion to participate is crucial. (Autio, 2022) Governance of digital ecosystems is underpinned by roles and responsibilities between actors. Private sector digital ecosystems have seen incumbents define an orchestrated governance reality, for example, big tech companies can leverage control over private platforms and data to act as orchestrators, essentially creating a first among equals effect as they exploit their unique positioning in a digital ecosystem to guide or steer developments, incentives, and structures. (Addo, 2022) The effects of orchestration in public sector digital ecosystems, on the other hand, are underpinned by an affinity to address societal challenges by exploiting the unique positioning of government as a maker of legitimacy, several participation incentives, and a source of authentic data. (Addo, 2022; Degen & Teubner, 2024) In the context of public digital identity ecosystems, government orchestration means taking authoritative decisions to strategically govern architectural alignment, creation of ecosystem incentives for participation, while balancing prevalent actor concerns and limitations in the ecosystem. (Addo, 2022) Empirical evidence on government orchestration of a national digital identity ecosystem in a non-EU federal country aligns with many governance challenges expected for the adoption of the EUDIF. Namely, challenges with stakeholder inclusion, ecosystem participation, and institutional arrangements. It has been found that open participatory architecture design enables the inclusion of outside stakeholder contributions to the outcomes of the system, such as technical component developers, enrolment agencies, identity attribute registries, and actors involved with testing, certification, and control of the solutions present in the ecosystem. Alignment of a national identity initiative with the existing digital public infrastructure has also been found to enable effective ecosystem governance, as the intervention could be strategically placed as a gateway layer between technical artifacts and public service delivery methods. Although this placement enabled a more effective and efficient public service delivery, ensuring the privacy of actors and constructing security and transparency controls were still critical factors of systemic success. (Addo, 2022) Orchestration can also create strategic negative incentives, effectively dismantling socio-technical structures that exploit gaps in governance to improve transparency and efficiency. (Addo, 2022) Moreover, control of intervention scope has enabled inclusion of a diverse stakeholder community, taking advantage of open architecture proposals to innovate on the ecosystem

to build identity assurance and authentication solutions, this control aspect has been underpinned by strategic decisions by policymakers to anchor and position identity as a gateway to access various programs managed under a shared national portfolio of digitalization, including but not limited to digital public services and support programs. (Addo, 2022) The intervention has carved out new methods of public service delivery that resonated with demands for the effectiveness of service delivery from both the demand and supply sides. (Addo, 2022)

The orchestration function can be executed towards multiple modalities of ecosystem governance. Digital ecosystems are formed around a digital core platform that facilitates actor, core platforms are often steered with standardization controls, a layer of participation incentives defines the frequency and modes of collaboration between actors to create ecosystem value, institutional mechanisms govern rules of interaction between participants to control the integration of the ecosystem value in a broader context (Autio, 2022) In terms of ecosystem architectures, scholars define three layers of digital ecosystems: technical layer that comprises of functionalities of participating platforms and methods of connectivity between applications, the activity layer, defining roles and relationships of and between participating actors and lastly a value layer to depict methods of value creation relationships and interactions that result in benefit extraction. (Autio, 2022) This perspective culminates in the description of top-down and bottom-up structuring of ecosystem orchestration. The top-down approach suggests that the essential blueprint design of value creation and implementation of incentives emerges from the orchestrator. The orchestrator executes this model to assign roles and responsibilities to actors to position their co-production value. Although top-down value constructs run the risk of having underdeveloped visions of ecosystem value for emerging ecosystems when creation of value rests upon other actors' acceptance of pre-ascribed roles and interaction dynamics. (Autio, 2022) Instead, value definitions may emerge from involved stakeholder negotiation, strategic placement of co-produced value in competition with incumbents' offerings; therefore, the formation of value models can be dynamic rather than fixed and implemented. To this recognition, an orchestrator can engage multi-stakeholder relationships and ecosystem participants to discover a proposed ecosystem architecture. (Autio, 2022) The discovery process both informs the categorization of ecosystem value as both 'offerings', meaning which services are central to value production, but the process also identifies roles and relationships attached to the

production of services. This perspective is especially salient where connectivity standards and specifications are open and the ecosystem is going through active development, underpinned by undetermined ecosystem roles and relationships. (Autio, 2022) In the early stages of ecosystems, orchestrators may strategize behavioural elements to elicit positive participation from ecosystem partners and the extending social fabric. This is crucial as critical network effects have not developed yet, urging early adopters, and promoting their stay by incentivising early adopter dynamics are found to be remedial strategies. Furthermore, reinforcing actors' roles and responsibilities through positive incentives is a condition that may ramp up the ecosystem pull effect in early stages. There can be a form of user and supplier contracts regarding data and connectivity. One of the most pressing issues is the introduction of new participants through early stages, often described as the 'chicken and egg problem'; alleviating this problem may take offering rewards, subsidies, and direct investment. To facilitate more participation, the ecosystem architecture blueprint may be open and participatory, enabling the creation of interfaces and technical artifacts to empower supply-side value generation. (Autio, 2022)

3.13 Value creation through information technology adoption in the public sector

Research suggests the relevance of information technology adoption and the creation of public value in governments. (Panagiotopoulos et al., 2019) In the public sector, the concept of value creation can be understood differently from the private sector. Public sector managers may have different goals and commitments to create socially driven value related to the outcomes of their actions. (Picazo-Vela et al., 2022) This concept of public value creation rests on the agreement between citizens and public managers on how management actions create value. Creation of public value through strategic governance has been linked to citizen participation, program effectiveness, and service quality. (Picazo-Vela et al., 2022) Conceptually, public value through information technology adoption can be generated as information technology integrates into public services as an enabler. (Panagiotopoulos et al., 2019) IT-enabled services offer the potential to incorporate specific values carried by the service stakeholder environment that can result in the reproduction of such values through IT-mediated public service interfaces. (Panagiotopoulos et al., 2019) Further conceptualization of public value in relation to e-government services has been offered. (Twizeyimana & Andersson, 2019) There, it has been suggested that creation of public value exhibits a multi-focal nature

that can stem from improvement of services, access to services, and underlying government functions and capabilities that supply the services. (Twizeyimana & Andersson, 2019)

3.14 Value creation through modes of collaboration in the public sector

Previous research suggests that organizational factors, inter-organizational collaboration, and enacted technologies have a significant effect on public value, with the most significant contributing factor being organizational factors. (Picazo-Vela et al., 2022) Moreover, a significant effect was discovered between organizational factors and institutional arrangements on enacted technologies, with variance in factors of enacted technologies being tied to variances in organizational factors, institutional arrangements, and inter-organizational collaboration. (Picazo-Vela et al., 2022) A significant effect on institutional arrangements and organizational factors is also posited by scholars, as well as a significant effect of institutional arrangements on inter-organizational collaboration, suggesting that organizational factors, inter-organizational collaboration, and enacted technologies carry effects on costs, productivity, transparency, effectiveness, and quality of behaviours that public organizations undertake. (Picazo-Vela et al., 2022)

3.15 Information technology governance in the public sector

Information Technology Governance (ITG) is a practice embedded discipline concerned with structures, decisions, accountability, procedures structures and activities to elicit desirable behaviour in using Information Technology (IT) (Wilkin & Chenhall, 2020) Contemporary definitions of the term utilizes a strategic lens to suggest that ITG defines procedures and mechanisms to monitor and make strategic decisions around IT and that such definitions can be a function primarily executed by executives or management boards to control IT strategy implementations and to ensure business alignment with IT objectives. (Pool et al., 2018) This perspective is furthered by suggestions that incorporate ITG in enterprise governance practices to fuse structures and processes together with IT objectives and business strategy. (Institute, 2003) Later definitions of the term further the priorities on strategy, business-IT alignment, and strategic management of Information Technology. As a result, the term has been uniformly understood as an executive function, exercised by a management board as part of the larger enterprise governance structures that defines, strategizes and implements processes, controls, structures and mechanisms

to enable business and IT alignment towards supporting organizational goals, controlling resources, measuring performance and to enable value creation through IT use. (Wilkin & Chenhall, 2020) Studies show that integrated ITG capabilities in organizations are demonstrated to enable human resources to further business processes or software (Debreceny, 2013) and introduce improvements to products, processes, and services. (Kim et al., 2011) Furthermore, enacting capabilities to ensure mature ITG practice is fundamental to the research stream, mainly to ensure business-IT alignment (Debreceny & Gray, 2013). As the field moves forward to embrace new technologies, it has been reported that organizational capabilities related to outsourcing (Liang et al., 2016) and inter-organizational arrangements have gained traction. (Rai et al., 2014) Scholars suggest that in the ITG context, value is created via cost management, improvement of organisational capabilities, and performance. (Wilkin & Chenhall, 2020) controls exist to improve value via ITG such as centralizing ITG strategy decision making for improved value creation settings, (Xue et al., 2011) delivering agility and adoption to improve organizational performance (Neirotti & Raguseo, 2017) ensuring organizational agility in uncertain value creation scenarios (Kohli & Johnson, 2011) ITG's role in intangible value delivery has also been demonstrated to improve organizational reputation and legal liability outcomes, (Günther et al., 2017) improve service delivery in industry generalizable ways (Smith, & McKeen, 2018) and specifically consistent and effective service delivery in e-government context (Gupta et al., 2008) as well as delivering process improvement capabilities. (Raschke & Sen, 2013) Use of ITG may be governed by enacted Key-Performance-Indicators (KPIs) to measure success, (Herz et al., 2013) its structures and mechanisms should be accountable (Ranganathan & Balaji, 2018) and auditable, (Chang et al., 2014) As a strategic function, board or management involvement in ITG has been found to translate into better contributions to organizational performance (Jewer & McKay, 2012) where strategies have been suggested such as creation of IT committees to centralize IT competency and steering authority within organizations. (Higgs et al., 2016) The topic of organizational risk awareness has been found to be a driver for business-IT alignment objectives. (Karhade et al., 2015) The capability to balance technical requirements derived from specifications and uncertain market conditions (Svahn et al., 2017) and business plans is especially relevant for ensuring business-IT alignment. (Berghout & Tan, 2013) From an organizational perspective, ITG interfaces with factors that are external to the organization, such as compliance and regulatory requirements, use of prescriptive frameworks and standards, while also being

influenced internally by external resources, organizational technical capabilities, resources, structures, and business processes. (Wilkin & Chenhall, 2020) Among these layered structures, ITG practice works to enable measurable, manageable, and aligned risk management controls and value delivery. (Wilkin & Chenhall, 2020)

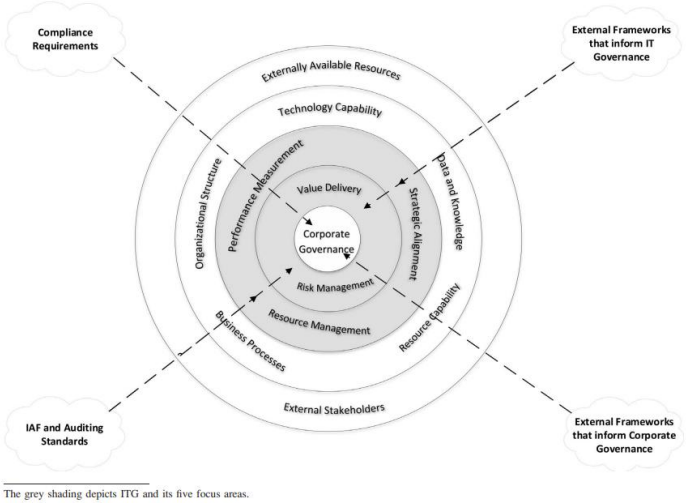

Figure 2 Conceptual hierarchies of ITG From (Wilkin & Chenhall, 2020)

The use and application of ITG in a public sector context has been underpinned by the use of common standards and frameworks such as COBIT (Control Objectives for Information and Technology), ITIL (Information Technology Infrastructure Library), and various ISO (International Organization for Standardization) standards. (Laita & Belaissaoui, 2017) Such frameworks aim to present straightforward process and activity descriptions to control IT resources, set targets for business-IT alignment, and enact measurements of performance. Importantly, such frameworks often offer capabilities to manage compliance requirements, enumerate best practices, offer a certain degree of compatibility with similar standards, and offer capabilities for service provider management. (Laita & Belaissaoui, 2017) As a common occurrence, such frameworks offer specific degrees of customizability to fulfill contextual objectives like managing IT investments. Beyond frameworks, it has been found that the practice of ITG in the public sector is categorically different due to organizational factors. (Laita & Belaissaoui, 2017) Public sector organizations may carry intangible goals, motivated to achieve efficiency to fulfill policy-driven missions, have lesser incentives for increasing productivity, have increased barriers due to legal and compliance constraints as well as bureaucracy, which in turn can influence organizational ITG via political influence. (Laita & Belaissaoui, 2017) It has been found that public sector organizational ITG is exercised in combination

with organizational-internal and external environments. Where structures, processes, and relational mechanisms enacted via ITG may translate into conceptually similar reflections on the organizational level. At the same time, the external environment of ITG practice may include culture, politics, interest groups, government, and citizens. (Laita & Belaissaoui, 2017)

3.16 Demonstrating design objectives from the literature

Following (Peffers et al., 2007) We conclude our literature review process by identifying a set of preliminary design objectives as a result of our survey of the direct and adjacent literature streams.

Preliminary design objectives	Design objective	Supporting Literature
1	Inform the technical implementation of digital identity solutions.	(S. Lips et al., 2020) , (Mahula et al., 2024)
2	Embed privacy and sovereignty principles in public sector business processes.	(Sedlmeir & Weigl, 2022), (Giannopoulou, 2023a)
3	Support EUDIW use-case formulation.	(Liesbrock & Sneiders, 2024), (Kolehmainen, 2021), (Laatikainen et al., 2025), (Degen & Teubner, 2024), (Weigl et al., 2023)
4	Offer compliance management capability.	(Laatikainen et al., 2025)
5	Inform process redesign	(Laatikainen et al., 2025), (Kölbel et al., 2022)
6	Support executive decision-making for EUDIF implementation	(Liesbrock & Sneiders, 2024), (Kolehmainen, 2021), (Laatikainen et al., 2025), (Kölbel et al., 2022)
7	Inform service design inputs.	(Korir et al., 2022), (Liesbrock & Sneiders, 2024), (Korir et al., 2022), (Lockwood, 2021)

Table 1 Design objectives derived from the literature Author's elaboration

4 Theoretical framework

We dedicate this section to introducing our theoretical framework of choice to offer an account of our thesis's use of the framework and extent of its application to the given problem environment. We use the Technology Organization Environment Framework (TOE) by Baker throughout this thesis to empower our analysis of the EUDIF as an adopted innovation and EUDIWs as adopted artifacts. (Baker, 2011) We posit that TOE provides a suitable theoretical lens for our design-driven study to map and depict external environmental factors and organizational factors as characteristics of a given technology to a given application context. Such application contexts are depicted in the TOE model as 'Technological Innovation Decision Making' states. The decision-making stage, as well as each entity dimension, depicts the interlinked and complex nature of technology adoption. The framework has been applied to similar problem contexts as ours in the past, especially in the Information Systems domain. (Baker, 2011) to look at organizational patterns of technology adoption (Kuan & Chau, 2001) and to scrutinize the role of IT governance in business contexts. (Olutoyin & Flowerday, 2016) Our use of the framework has enabled the creation of a level of analysis patterns developed during our data analysis and coding processes. The framework was eventually consulted at artifact design stages as we attempted to propose structures for EUDIW activities, controls, and processes from an organizational lens, depicting an environment external to the EUDIW implementation, an organizational structure of EUDIW implementation, and technology characteristics in an integrated and linked fashion. In sum, the use of TOE informs the hierarchies of organizational knowledge as well as actor relationships explored in this thesis.

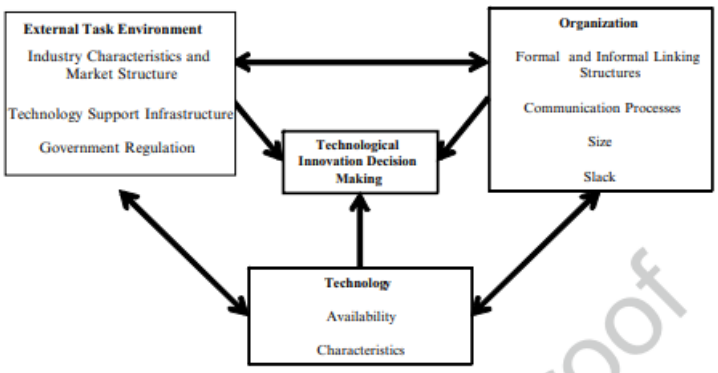

Figure 3 The Technology Organization Environment (TOE) Framework From (Baker, 2011)

5 Research Design

We dedicate this section to introducing our research methodology. This chapter will include an introduction to our research methodology and its application, as well as our strategy for data collection and analysis. Basic features of our research conform to the outlines of empirical research in the information systems domain conducted via qualitative data collection means in the form of semi-structured interviews, deriving its basis from practical challenges in the field in order to generate applicable insights in the form of reference materials for the application domain and its stakeholders. (Benbasat & Zmud, 1999)

5.1 Methodology

Throughout this thesis, we apply the seminal methodology of design science research introduced by (Peffers et al., 2007) and further described by (Brocke et al., 2020) and (Hevner et al., 2020) As a result, our thesis exhibits multiple characteristics such that its problem definition and research motivation have been inferred from a relevant problem domain. (Peffers et al., 2007) A solution towards the identified problem has been expressed in solution objectives that are defined in the theory of the applicable domain. Subsequently, such solution objectives have been expressed in a designed artifact towards addressing a practical problem. (Peffers et al., 2007) The generated design knowledge has been put through multiple stages of demonstrated rigor by iteration as we apply it to the original application domain. Analysis of the accumulated design knowledge that has been derived as a result of rigorous iteration rounds on such an artifact leads our research to come up with a final designed artifact that exhibits and fulfils a set of identified solution objectives (Peffers et al., 2007) Using the DSRM as a blueprint, we will attempt to lay out and visualize our use of the methodology in the continuing sections of this chapter.

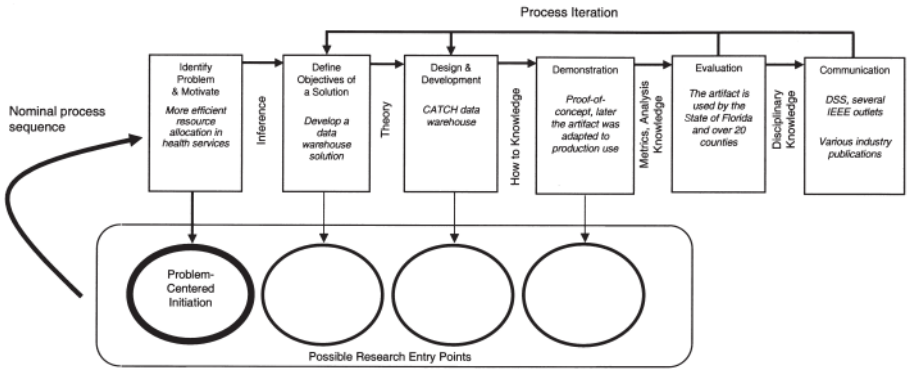

Figure 2. DSRM Process for the CATCH Project

Figure 4 DSRM process From (Peffers et al., 2007)

Our use of the DSRM process starts with a problem-centered research entry point as classified by (Peffers et al., 2007) We elaborated that the concrete implementation and adoption targets imposed on the European public sector institutions presented a problem for the public digital identity systems governance domain. While elaborating, we employed a prescriptive lens towards the problem space, deriving insights from solution design theories and entities situated in respective solution environments. (Brocke et al., 2020) Moreover, following the conceptual model of DSR projects, we defined sub-components of context and goodness criterion for our approach, situating them in domain, stakeholder, time, and space contexts as well as dimensions of technology and socio-technical interactions. (Brocke et al., 2020) Further, we derived further motivation towards developing a solution-based study by investigating the relevant academic literature to gain conceptual depth towards addressing practical problems. A general result of our motivational investigation has led our study further to scrutinize the problem space from the lens of governance, as it has been a uniformly recurring theme in the literature. We initiated a literature review process to initially survey and generate a preliminary list of relevant solution objectives towards addressing the identified and motivated problem. Subsequently, moving onto the design stages, we have conducted a round of expert interviews spanning multiple actor roles that were identified in the problem space by scholars; results from the interviews have been used to either justify or annul the initial set of solution objectives. (Peffers et al., 2007) Following the conclusion of the solution objective evaluation round, we scrutinized various possible design pathways, methods, and models towards a designed solution (Brocke et al., 2020). At this stage, our consultation of instantiated governance models and governance methods in the literature led us to derive high-level requirements for the governance model. We then

designed and demonstrated an initial governance model artifact built according to and in order to fulfil an empirically validated set of solution objectives. (Peffers et al., 2007) Finally, we performed an evaluation iteration round on the governance model artifact with additional design insights derived from a final round of expert interviews, resulting in the final form of the demonstrated governance model artifact in this study's results chapter. We also offer a process model that has been constructed using the ArchiMate modelling language, of our study's utilization of the DSRM below for reference.

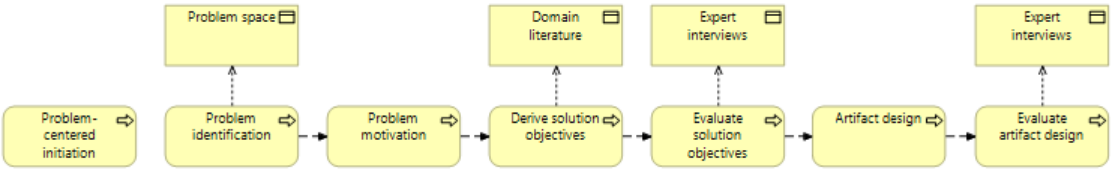

Figure 5 ArchiMate process model of our DSRM research process Author's elaboration

5.2 Literature review methodology

We chose Web of Science Core Collection and SCOPUS as suitable catalogues for our literature review based on their capability to return extensive academic literature on information systems and public governance research streams. We performed our querying process in multiple steps. (1) We have only included results in the English language, (2) Only peer-reviewed articles, conference papers, and peer-reviewed academic book chapters were included. (3) We used the built-in filtering systems of SCOPUS and Web of Science Core Collection to filter for temporal and contextual accuracy. Moreover, direct query results were filtered only to return results in related disciplines (Webster & Watson, 2002), such as information systems and public governance. Lastly, articles demonstrating purely technical concepts or empirical studies with narrow, sectoral-dependent focuses were excluded. We employed a single iteration of forward and backward searches (Webster & Watson, 2002).. Our preliminary search resulted in 297 results, which were manually screened for title, keyword, and abstract relevancy. In total, 40 papers were selected. Our backward search identified three articles eligible for addition following title, keyword, and abstract readings. Our forward search concluded with two additional eligible articles. In total, out of 297 initial results, we have included 40 articles, with five additionally eligible articles resulting from the backward-forward search process. Following search queries were generated by the authors and subsequently executed against the selection of search engines: 'digital identity wallet AND public

sector', 'digital identity framework AND governance' and 'digital identity ecosystem' Following (Webster & Watson, 2002) we attempted to include articles from adjacent research domains such as digital ecosystems, cross-border services, public digital infrastructures etc. Subsequently, we have generated a concept map of our literature survey that has been attached to the appendix section accessible at Annex A. Further, we provide a PRISMA diagram of our literature survey attached to the appendix, accessible at Annex C.

5.3 Data Collection

In this section, we will outline our thesis's approach to collecting empirical data, selection of data sources, and we will offer justifications for our data collection methods.

Our problem motivation has motivated this thesis's approach to data collection in terms of defining the focal point of organizational perspectives as the level of analysis. We utilized the conceptual model of digitalization practices introduced by Göran to further inform and detail our approach to empirical data collection. The model suggests that in such an environment as our choice of solution space, interactions between digital artifacts and institutional actors happen in co-existence with humans' personal and inter-subjective knowledge. (Göran, 2019) Considering our use of DSRM methodology, which the same scholar has also recognized as a practice-based design study. We ascertained to collect data from a multitude of actors to inform our design knowledge accumulation process. Including individual actors in interaction with a digital artifact, representatives of an institutional perspective that have been in interaction with other institutional perspective representatives, or have been in interaction with the technology themselves. Furthermore, in order to further contextualize such classification of actor perspectives, we utilized a conceptual model of actors in the EUDIF ecosystem developed by EUDIF ecosystem researchers. (Degen & Teubner, 2024) They utilized a three-type stakeholder classification for an ecosystem study on EUDIF governance. Identifying private and public sector businesses, public administrations, and regulators, as well as civil society and community groups in the EUDIF ecosystem. (Degen & Teubner, 2024) Building on top of their classification, we have developed an adapted elaboration of ecosystem actors that forms the basis of our actors' classifications. We generated a graphic of our elaboration of EUDIF ecosystem actors as an appendix entry in Annex D. We elected to conduct semi-structured interviews for data collection, as the collection method has been

previously demonstrated in related research streams to uncover perspectives and experiences of participants in fields exhibiting knowledge fragmentation. (Weigl et al., 2023) Following the questionnaire design, we conducted a total of 28 semi-structured interviews. Interviews took place online via the Microsoft Teams platform between March and May of 2025, and each interview was attended by a single subject matter expert with no repetition of experts. After the interviews were concluded, the process resulted in a total of 1026 minutes of transcribed text that were obtained by automated means and have also been checked by the author for accuracy. We conducted interviews in two stages, first stage included 18 expert participants spanning private sector entities: in specific: data issuers, wallet relying parties and ecosystem service providers such as wallet providers, intermediaries, brokers and trust service consultants, public sector institution representatives, in detail: wallet relying party and data issuer organizations in multiple Member States including regulatory organizations, representatives of NGOs, digital public infrastructure providers and independent digital identity researchers were also included in the first round of interviews in order to validate literature derived solution objectives. For the second round, a similar composition of expert participants was included in the phase to evaluate the first iteration of the designed governance model artifact. Throughout the data collection process phases, interviewees were selected according to their own and organizational roles as well as their domain expertise. Individual roles of participants were identified via online job boards or online biographies, while we actively asked participants to reveal their organizational roles during the interviews in order to ensure that our expert pool exhibits diversity. During interviews, we consider experts to possess relevant and factual knowledge about their role, organizational role, and dynamics of the EUDIF ecosystem, as well as dynamics of related concepts from an organizational perspective. (Mergel et al., 2019) We strictly utilized snowball sampling (C. Parker et al., 2019), where we asked participants to recommend suitable direct contacts to conduct interviews with, going forward, to build our final composition of experts. We followed a thematic saturation lens (Marconi et al., 2016) to decide when to conclude the data collection process by employing a thematic analysis matrix of interview data to track expressed interview themes over the span of the entire collection process in order to arrive at saturation observations. (Saunders et al., 2018) We observed that for the first stage of data collection, thematic saturation was exhibited at the 18^{th} observation, while for the second stage of data collection, the evaluation stage saturation was exhibited at the 10^{th} observation. We found that such

numbers corroborate with observations from the literature. (Marconi et al., 2016) In terms of interview design, questionnaires were designed according to each role's expertise and involvement mode in the EUDIF ecosystem. (Myers & Newman, 2007) We iterated on the design of the questionnaires in order to further accommodate the verbosity of the data collected according to feedback gathered by participants. A table of thematic observations of semi-structured expert interviews has been generated for reference in the appendix section of our thesis at Annex F. Furthermore, another table of interview partners, including their organizational and personal roles as well as details about interview instances, has been generated in the appendix section of our thesis at Annex E.

5.4 Data Analysis

In this section, we will outline and describe our approach to data analysis. Throughout our data analysis, we have made use of qualitative coding methods to analyse interview data. (Weston et al., 2001) We employed a self-developed and inductive coding system during the coding process. We developed coding patterns in line with OAS (open-axial-selective) coding techniques owing to their prominence in the information systems research domain.(Alhassan et al., 2023) During our data collection phase, we collected a total of 1026 minutes of interview extracts, such data mostly conformed to specific patterns of directional statements in the form of one representative of a pre-defined ecosystem role making statement(s) about perceptions, roles, responsibilities, or activities of another ecosystem role bearer. Hence, we employed an OAS coding pattern to further uncover, depict, and demonstrate the effects of directionality and actor roles in the interview data pool. Firstly, we employed open coding, in which we attached various descriptors such as perception, challenge, barrier, or driver to statements to cluster observations towards common themes. Secondly, we employed axial coding patterns on top of existing open codes to further uncover related themes (Corbin & Strauss, 2014), attaching directionality markers between statement subjects and statement objects according to pre-defined ecosystem roles. Attaching directionality helped us to establish frequencies of common ecosystem and organizational level challenges, barriers, drivers, and perceptions expressed between ecosystem actors, underpinning priority themes, concerns, and common challenges expressed in concert. Such themes were especially prevalent during the evaluation of solution objectives. For further reference, we developed a code frequency distribution graphic that depicts the frequency of axial codes between ecosystem actors, helping to visualize frequencies of observations that were

made by different ecosystem actors. This graphic has been included in the Annex G. During the coding process, the qualitative data analysis tool NVIVO has been used to come up with a single coding scheme, including open and axial codes. The codebook has been supplied along with the thesis appendix and has been included in Annex H. As a result of our coding process, a total of 600 open codes and 290 axial codes have emerged. The distribution and description of codes have been made available to readers as an attachment to our thesis.

5.5 Case study

This thesis extends a case study lens to the EUDIF implementation contexts of Belgium and the Netherlands due to the contemporary and undertheorized nature of the problem space. (Benbasat et al., 1987) The multi-actor setting of the EUDIF ecosystem enables us to fit our research goals on a case study focal point to examine the phenomenon of implementation governance in the selected two EU Member States. In this section, we will describe our approach to constructing a case study and offer justifications for its configurations. This section will be followed by brief background descriptions of each country in order to provide ample context to the audience. Firstly, following (Benbasat et al., 1987), we define our unit of analysis as entire organizations specifically undertaking EUDIF implementation activities. Differences have influenced our case country selection in EUDIW rollout approaches at the time of this research. Belgium aims to centrally develop and offer a government-driven digital identity wallet solution as a building block for public sector use cases. (Interviewee 9) There has been limited interest so far in allowing private sector third parties to interface and integrate with the Belgian EUDIW prototype. On the other hand, the Netherlands aspires to integrate private sector use-cases in a government-provided digital identity wallet solution (Interviewee 7), with the possibility of private certified wallets being used in public and private sector use cases. (Interviewee 14) Such approaches are classified in the literature as two very distinct cases of EUDIW rollouts. (Degen & Teubner, 2024) By selecting two cases, we aim to make our design knowledge approach more comprehensive, enabling our model to inform governance aspects of both rollout approaches. We posit that our approach may enable the generalizability of our findings towards other Member State contexts, as EU-wide Regulatory frameworks form the basis of compliance and digital identity solution designs. However, organizational implications of implementation may ultimately differ on a case-by-case basis for each Member State.

5.5.1 Case background Belgium

In this section, we introduce the digital identities landscape in Belgium from a governance and adoption perspective. Belgium is among the pioneers of electronic identification in the European Union. Policy formulation and development of an identity strategy began in 1999 with the establishment of a commission tasked with establishing an e-government policy and surveying opportunities and challenges. (Mariën & Van Audenhove, 2010) Following the approval of the feasibility study on electronic identification by the Council of Ministers in 2001, a private company was chosen as a Certification authority to deliver electronic certificates to electronic identification cards containing a chip to enable secure signing and online authentication. (Mariën & Van Audenhove, 2010) Another private company was assigned to the role of the producer of the electronic identity cards. (Mariën & Van Audenhove, 2010) Belgium did not face significant challenges in the citizen adoption domain with the electronic identification scheme. Furthermore, digitally capable features of the electronic identification means were delivered on an opt-out basis, requiring express will from users to deactivate electronically enabled functionalities. (Mariën & Van Audenhove, 2010) The card was seen as both an identification method and a service delivery means by policymakers. (Mariën & Van Audenhove, 2010) A unique National Registration Number from the national register databases is supplied with every electronic identity card. The reuse of the unique identification number establishes the basis of authentic source access for the Belgian authorities. Access is controlled by a privacy commission to oversee and authorize all kinds of data exchanges containing personally unique identification attributes. (Mariën & Van Audenhove, 2010) The exercise of the steering power of the privacy commission can be seen as strict, favouring data minimisation and minimal disclosure practices, which can be limiting for private sector use cases over authentic data reuse. (Mariën & Van Audenhove, 2010) As a federal European state with clear delineation of responsibilities regarding distribution of competencies and electronic identity management mandates, currently, identity management is situated at the federal level, while e-government competencies are regionally managed. Resulting from delineation structures, regional and local entities are empowered by law to develop and implement applications accordingly including their oversight ability on design objectives, conceptual frameworks and financial means, (Mariën & Van Audenhove, 2010) this aspect may have resulted in a fragmented catalogue of eID capable public services with regional and federal authentication

platforms have been enacted in co-existence (Interviewee 8) This service fragmentation can also lower incentives for cooperative service provision and delivery as clear mandate definitions can introduce budgeting and funding challenges as well as a drive for increased sovereignty in service provision decisions. (Interviewee 8) As a result, e-government services are scattered across regional borders with fading relevance towards residents of other regions. (Mariën & Van Audenhove, 2010) Belgium provides identity lifecycle events from a variety of public sector bodies. For example, citizens engage with municipalities to manage the reissuance of identity cards, while regional, local, and federal databases may store authentic data on citizens. (Mariën & Van Audenhove, 2010) Despite being a pioneer in the domain and facilitating factors, electronic identity use has not been found to be used frequently; these factors are connected to stringent privacy controls over authentic source data reuse.

The Belgian Federal Government utilizes the competencies of BOSA. The Federal Public Service for Policy and Support (Interviewee 8). This organization has been responsible for polices around digitalization and simplification across multiple federal public services as a provider of building blocks that other federal public services can use and integrate. (Interviewee 8) While a clear separation of roles and mandate areas has been a defining principle in Belgian eIDMS governance. (Interviewee 8) Recently, other public service operators have been encouraged federally to reuse building block components provided by the horizontal public service, hence acting as a driver for architectural centralization in the Belgian government. (Interviewee 8) BOSA's competencies as a centralized provider of technical and security architecture, as well as digitalization policy, have become more important recently as the federal services have been tasked with developing the Belgian EUDI Wallet offering. (Interviewee 9) Other federal public services, such as SPF Economy, hold the supervisory body role for electronic trust services, and SPF Interior carries competencies in issuing digital identity cards. (Interviewee 9) The Federal Authentication Service (FAS) allows citizens and businesses to authenticate to digital public services in Belgium. This middleware can be used with an electronic identity card or other recognized private or cross-border means. (Interviewee 9) As identification is a federal competency, this service is offered to other Belgian public sector organizations. As a result, via FAS, the federal public service is the convergence point and effective broker of digital identity transactions in Belgium. While regional and local governments in Belgium may offer the EUDI wallets to citizens and businesses as an identification

means (Interviewee 9), the reuse of the federal public service competencies and technical components is more likely to materialize.

5.5.2 Case Background Netherlands

The Netherlands is an advanced country in terms of the digital identity landscape, diversity, and maturity of service offerings and individual digital identity service adoption rates. (S. Lips et al., 2020) At the moment, the Dutch public and private sectors are served by the eHerkenning trust framework for businesses and DigiD for individuals. DigiD, which is operated by an affiliate organization of the Ministry of the Interior and Kingdom Relations, enables citizens to authenticate with government service portals and access digital public services. (S. Lips et al., 2020) The Dutch public sector also has a well-developed practice of information sharing for service delivery. (Bharosa et al., 2020) Similar to the Belgian case, a clear delineation of competencies and responsibilities towards digital identity service provision exists. At the moment, several Dutch Ministries and specialized ministerial organizations are collaborating to develop the national digital identity wallet (Interviewee 7). Local governments, such as municipalities, are empowered to design their approach for EUDIW use and EUDIF use. (Interviewee 15) We found evidence that the Dutch digital identity wallet may incorporate private sector use cases from the start, in contrast to the Belgian EUDIW initiative. (Interviewee 7) Similarly to the previous case, the concept of Federated Service Connectivity exists in the Netherlands. (Interviewee 14; Interviewee 15) This architectural middleware enables public sector organizations to share data between each other and through other Member States using the OOTS gateway in the Netherlands. (Interviewee 14) It also enables the use of common standards for connectivity (Interviewee 15) and delegation, as some public sector organizations may depend on private sector entities while fulfilling their mandates. (Interviewee 15) Furthermore, similar to Belgium, a unique citizen identity number, BSN (citizen service number), exists in the Netherlands, which acts as an entry point for accessing public services. (Interviewee 14) In the Netherlands, authentic data for individuals can be in the custody of National governmental entities and local governments, and some data attributes can be jointly owned by more than one entity. (Interviewee 14)

6 Results

Following (Peffers et al., 2007) We dedicate this section to describing our results. We will structure our description of our results in multiple parts: Firstly, we will be demonstrating the initial design science cycle iteration, where we evaluate design objectives for a governance model artifact through 18 semi-structured expert interviews. After the demonstration of the evaluation round, we will present a second iteration of the design objectives. Secondly, we offer a description of and methods for the operationalization of every design objective in an ITG modelling context. Before modelling takes place, we follow. (Alismail et al., 2017) To define modelling constraints and criteria to evaluate the goal fulfilment of the governance artifact, therefore concluding the first iteration cycle of DSRM. In the second cycle, we will demonstrate a cycle of expert evaluations, executed in the form of semi-structured interviews with 10 experts to evaluate the fit and success of the first iteration of the governance model artifact. We derive several design changes from the expert evaluation. Afterwards, we incorporate design changes into the modelling context to come up with the second and final iteration of the governance model artifact. As the final step of the second DSRM iteration cycle, we offer a description of the artifact and demonstrate artifact constraints and goal fulfilment levels.

6.1 Design Science Cycle First Iteration

Following (Peffers et al., 2007) We dedicate the following chapter to the demonstration of our first DSRM iteration, where we evaluate design objectives with subject matter experts, offer an evaluated set of design objectives, and present and justify the modelling context for the proposed model artifact. We will conclude the first iteration with the modelling of the first iteration of the governance model artifact.

6.1.1 Evaluating design objectives

Following our data analysis of the first iteration of interviews to derive design objective evaluations for a governance model artifact, we generated 600 open and 290 axial codes. Each pertains to a reported or perceived issue area, collected from different ecosystem roles. In this section, we will offer an analysis of prevalent themes and current governance gaps resulting from our data analysis. Firstly, following the EUDIF ecosystem conceptual model by (Degen & Teubner, 2024), we generated a blueprint of ecosystem actors and

mapped our axial codes between different actors to represent the directionality of findings. This approach enables us to demonstrate the self-determined capabilities of public sector organizations. While also enabling capability gap discovery, as expectations of capability building from other ecosystem actors are mapped towards public sector organizations. A figure that incorporates axial code distributions from the first evaluation interviews has been generated and supplied in the Annex G. During our analysis solution providers have strongly iterated the economic benefits, (Interviewee 1; Interviewee 22) user friendliness (Interviewee 1) process efficiency gains potential for the use of EUDIW capabilities and use of EUDIF recognized artifacts such as EAAs in business processes (Interviewee 1; Interviewee 24), Solution providers have elicited the importance of use-cases and existence of clear business value for EUDIW adoption (Interviewee 2; Interviewee 4; Interviewee 8; Interviewee 13), and recognized Know-Your-Customer (KYC), (Interviewee 1; Interviewee 2; Interviewee 4; Interviewee 8; Interviewee 13; Interviewee 22) and reducing compliance needs via wallet adoption (Interviewee 24) as potential use cases. A service provider posited that certain use cases carry a higher value to ramp up adoption, potentially. (Interviewee 24) While service providers reiterated the importance of business models, they also recognized the payment intention behaviour for ecosystem services as one of the key challenges (Interviewee 8; Interviewee 3).

Service providers also point out that the critical value propositions of the EUDIF ecosystem are the reuse of authentic data in processes (Interviewee 1; Interviewee 2; Interviewee 22; Interviewee 24; Interviewee 26), eliminating the need for manual verification and potentially increasing procedural efficiency. Privacy-preserving features for users (Interviewee 1), increased security as well as data and identity assurance for business processes (Interviewee 1), clear legal liabilities for transactions (Interviewee 3), (Interviewee 4; Interviewee 24), Most service providers posit that value cases for the wallet primarily exists in business-to-business domain. (Interviewee 2; Interviewee 8; Interviewee 24). On the topic of individual wallet adoption, the lack of use cases is identified as a barrier. In contrast, well-defined use cases with high use frequencies represent a clear driver for adoption (Interviewee 5; Interviewee 16), alternative methods of identification can also challenge individual wallet adoption (Interviewee 24; Interviewee 25), Moreover, for individual use cases offering more convenience and security towards everyday transactions via wallet use cases can be an adoption driver (Interviewee 24) Complexity of use attached to wallets without clear benefits has been

identified as an individual adoption challenge. (Interviewee 22) The role of individual trust in the government has also been identified as a dimension of individual adoption (Interviewee 26). The concern of unintentional data over-sharing is evident, as service providers suggest the wallet can be an additional source of liability for the public sector. (Interviewee 24; Interviewee 25; Interviewee 26).

Service providers recognize a lack of concrete business value and well-defined EUDIW use cases as the primary barrier to ecosystem value creation and participation. (Interviewee 2) Others recognize low levels of actor awareness (Interviewee 4; Interviewee 6; Interviewee 25), from governments which have been tasked with interfacing with EU-level decision making, wallet development, and ecosystem rollout, effectively exercising orchestration capacities. On the topic of orchestration, service providers expect development of certification schemes for trusted products (Interviewee 5; Interviewee 22), standards (Interviewee 13) help for defining wallet-based business models (Interviewee 13) development of harmonized requirements for service providers (Interviewee 6) programs for direct engagement of service providers (Interviewee 6; Interviewee 24) from Member States. Some service providers argue that government orchestration capabilities may be challenged in the Netherlands and Belgium, as each government layer has a say on how and whether to implement EUDIF, complicating national-level governance and making implementation. (Interviewee 8) Overall, service providers tend to favour a market-based approach to EUDIF ecosystem enactment, where the orchestration role of the government is to develop rules, guidelines, specifications, and standards while actively procuring from the market.

According to service providers, ecosystem actors' readiness for wallet adoption is challenged by significant scale changes in business processes and business ecosystem to adopt EUDIWs (Interviewee 2), especially in ecosystem infancy where low ecosystem maturity may elicit hesitancy from prospective participants to assess ecosystem value (Interviewee 8; Interviewee 24), They recognize that high compliance requirements, (Interview 2; Interviewee 8), Fast-changing regulatory landscape (Interviewee 6; Interviewee 8), non-harmonized standards for authentic data source access (Interviewee 4) and wallet capabilities of data sharing being incompatible with business models of registries (Interviewee 13), (Interviewee 24; Interviewee 25) creates important barriers for ecosystem participation. Moreover, service providers mention challenges of collaboration and interfacing with public sector entities, national legislations may be

found to be not in alignment with EUDIF requirements (Interviewee 4; Interviewee 6), and unclear public procurement processes and introduce innovation bottlenecks (Interviewee 6)

Service providers perceive the availability of PID capabilities in wallets as a chicken-and-egg problem, positioning PID availability as a driver for further credential adoption. (Interviewee 5; Interviewee 8; Interviewee 22; Interviewee 24), While also recognizing the central role of the government to develop and provide PID capabilities to the wallet (Interviewee 8) They suggest that wallet adoption needs internal stakeholder support (Interviewee 3) Importantly, service providers suggest that process redesign is an important step to ensure digital capabilities of the wallet can transform analogue modes of process design thinking, (Interviewee 3; Interviewee 4), which have been found to be non-privacy friendly, (Interviewee 1) not efficient (Interviewee 1; Interviewee 24), they posit that process redesign can enable new business models or cases (Interviewee 4) However, there is almost an unanimous statement that technical implementation of the EUDIF does not represent the main challenge against ecosystem success. (Interviewee 3; Interviewee 4; Interviewee 5; Interviewee 8; Interviewee 25), Instead, service providers point to governance challenges (Interviewee 8; Interviewee 5; Interviewee 22). Service providers also recognize the chicken-and-egg problem of early EUDIF ecosystem configuration in terms of technical component availability, suggesting that availability of attribute validation capabilities for relying parties may ultimately positively impact EUDIF adoption metrics by organizations. (Interviewee 8) Another challenge exists for ecosystem participants wanting to bootstrap technical solutions, while a market for them does not exist yet. (Interviewee 24) Interviewees recognized the political effects on ecosystem development and harmonization (Interviewee 8) at the same time, service providers recognize the role of established identity management capabilities in their respective governments to be a driver for adoption (Interviewee 8) However, high maturity of state eIDMS can also be an adoption barrier for the wallet as alternative and potentially more salient methods of identification are available (Interviewee 16), (Interviewee 26) nonetheless, wallet is of importance for cross-border use cases as cross-border users of digital public services will not have their attributes stored nationally (Interviewee 26; Interviewee 16).

Service providers carry ecosystem-level concerns, including a common perception of governments' exclusive focus on compliance targets (Interviewee 3; Interviewee 4;

Interviewee 8; Interviewee 19; Interviewee 25), and non-alignment between running programs on cross-border digital identities. (Interviewee 19) For some, there is evidence that service providers may believe public sector carries an ecosystem-level drive to adopt a 'bare-minimum approach' when it comes to EUDIW adoption (Interviewee 26) due to high costs associated with required digital transformation efforts (Interviewee 2; Interviewee 25), or challenges with harmonizing technical specifications to enable data flows in the ecosystem (Interviewee 4) Moreover, as most of the authentic data of wallet users is already available to the government. A provider suggests that government process change may gradually happen as wallet holders begin to accumulate value-added credentials in their wallets needed by government processes that cannot be acquired by other means. (Interviewee 25) There is a perception among service providers that the public sector will be incentivized to opt for buying wallet solutions from service providers instead of building them or reusing technical components. (Interviewee 5) Moreover, wallet adoption for relying parties has been tied to the existence of mass adoption. (Interviewee 24) Service providers typically agree that organizational transformation towards EUDIF readiness stems from business process redesign capabilities (Interviewee 3; Interviewee 4; Interviewee 5), However, they voice concerns against process digitization and change in the public sector being a highly regulated field (Interviewee 5; Interviewee 8), as a result, one Interviewee suggested that organizational digital transformation should start with understanding compliance requirements and pay attention to legal constraints for process redesign. (Interviewee 8)

Public sector organizations perceive unclarities in the pan-European governance framework in terms of availability of certification schemes (Interviewee 6) fast-paced nature of regulatory developments (Interviewee 9), unclarities in conceptual constructs of the EUDIF ecosystem such as role definitions of ecosystem actors (Interviewee 15; Interviewee 18), Most public sector representatives recognize their organization's readiness as authentic source operators and data providers as low. Citing immature standardization and regulatory developments around regulated data provider ecosystem roles for reasoning (Interviewee 7; Interviewee 9; Interviewee 14), nonetheless, public sector representatives, similar to service providers, underline the importance of well-defined use cases and value stream formulations for wallet adoption. (Interviewee 14)

Like service providers, public sector representatives recognize economic benefits of the EUDIF ecosystem, (Interviewee 10) wallet data sharing capabilities, (Interviewee 10),

they suggest using the wallet as a digital transformation catalyst (Interviewee 11; Interviewee 12), wallet's capability as an offering to public sector entities to meet data and access compliance targets (Interviewee 14; Interviewee 21), They might also find value in ecosystem service scope extensions to include payment authorization and electronic signatures for mobile signing. (Interviewee 10) Representatives reiterate the reuse of authentic data as a driver for efficient business processes in the public sector. (Interviewee 10; Interviewee 11; Interviewee 14; Interviewee 21), Moreover, EUDIWs' role as a pan-European public digital trust medium towards public service delivery has been voiced (Interviewee 12). The Public sector perceives wallet security as a paramount concern, and they are likely to expect increased attention paid to wallet security assurance. (Interviewee 7; Interviewee 12), Lack of clear incentives in the public sector domain for digital transformation around EUDIW objectives has been identified as another barrier. (Interviewee 11) The public sector representatives also recognize Member State competencies with managing eID means, having a mature eID culture, and authentic source management as an enabler for ecosystem development capability of a given Member State. (Interviewee 9)

Public sector organizations may diverge on their observations of the dynamics of private sector participation in the EUDIW ecosystem. At the same time, some organizations recognize private sector participation as a key adoption driver in terms of the frequency of use of digital identity wallets towards private sector use cases, which is known as an adoption driver. (Interviewee 6; Interviewee 12), They also perceive that the reuse of authentic data by the private sector may function as a business enabler (Interviewee 6; Interviewee 14). Different public sector stakeholders tend to support the availability of multiple recognized wallets instead of a single government-provided wallet, which might constrict available use cases and user choice. (Interviewee 10) Similarly, the multiplicity of wallet choices might increase individuals' trust in the ecosystem (Interviewee 10). Other representatives voiced priorities towards completing their primary mandate to develop, launch, and supply PIDs to the EUDI wallets before reaching out to private sector organizations. (Interviewee 9) Availability of PID capabilities has once again been recognized as a critical use case catalyst, an ecosystem-level first step to enable users to acquire more credentials. (Interviewee 12) Representatives also posit that procedures for relying party operations as defined in the ARF and EUDIF may not be mature enough to take concrete steps at this time; hence, in many public sector organizations, no EUDIF

rollout for private sector relying party use towards the wallet has been planned. (Interviewee 9) Similarly, guidelines for business process change or use case definition have not been in the works for public sector organizations (Interviewee 9), which might constrain wallet use cases to what is immediately possible within the existing organizational context at the relying party side. On the other hand, comprehensive legal constraints around business process redesign can limit the availability of public sector wallet use cases. (Interviewee 14)

Public sector organizations posit clear mandate and responsibility delineations on responsibilities on EUDIF rollout in their respective countries, (Interviewee 6; Interviewee 15; Interviewee 17; Interviewee 23), For some, definition of mandates and roles may complicate the EUDIF adoption pathways by further constraining the role and relationship prerogatives in the ecosystem (Interviewee 11) Furthermore, public sector representatives identified organisations other than their own to be in lower levels of awareness regarding their obligations towards supporting EUDIF (Interviewee 6; Interviewee 11; Interviewee 23), Multiple interviewees have corroborated to a lack of a uniform roll-out plan, vision or centralized initiatives for EUDIW adoption. (Interviewee 9; Interviewee 15; Interviewee 17), Many representatives have recognized the multi-level governance aspect of EUDIF in the Dutch, Belgian, and, to some extent, German public sector as a major adoption challenge, as every data owner organization has to be adopted into the ecosystem separately. (Interviewee 10; Interviewee 11; Interviewee 17), More specifically, representatives recognize each entity's decision-making sovereignty over budgeting and implementation within the boundaries of applicable laws. (Interviewee 17) Concerns have been raised in terms of different capabilities in different levels of the public sector for implementing EUDIF, which might pose additional challenges. (Interviewee 11; Interviewee 15), At the same time, public sector obligation to support EUDIW has been identified as a potential ecosystem catalyst (Interviewee 10). Representatives also suggested the role of administrative culture and attitudes as a relevant dimension for organizational EUDIW adoption. (Interviewee 12; Interviewee 21).

Public sector representatives recognize multiple capabilities of the wallet associated with public value creation. Specifically, motivation has been identified to utilize data minimisation and privacy friendly capabilities of the wallet to support organizational objectives and legal mandates (Interviewee 6), (Interviewee 21) Public sector

representatives also recognize intangible benefits of enabling the use of the wallets such as giving individuals control over their data. (Interviewee 6), (Interviewee 14), (Interviewee 21) Privacy-preserving wallet capabilities have also been linked to unique value propositions of the wallet ecosystem and basic digital rights of citizens. (Interviewee 10), (Interviewee 14) rolling back of bureaucracy as well as complex government processes. (Interviewee 17) safety, trust and confidentiality of data (Interviewee 17) and use of baked-in consent mechanisms via wallets. (Interviewee 17) However, representatives posit that full adoption of the EUDIF may necessitate rethinking of public sector business processes around EUDIW capabilities. (Interviewee 11), (Interviewee 14) Compared to service providers, public sector representatives have had a higher propensity to have a granular overview on technical readiness challenges towards EUDIF adoption. Relating challenges to chances in business processes and technical infrastructure management to support EUDIW use cases. (Interviewee 14) Moreover, EUDIW readiness may spell out more work towards architectural development as authentic sources, intermediaries and issuers in each Member State must use common channels of connectivity. Resulting in fragmentation in architectural baseline. (Interviewee 15) Data access and workflow concerns have been tied to constraints introduced by legal frameworks as well. (Interviewee 15) Interviewees have also pointed how the medium of EUDIW service delivery should be structured, they posit that a consistent, digital-first, coordinated and gradual service delivery must be enacted to ensure user trust in wallet driven public business processes. (Interviewee 17) On the topic of service design, governments should ramp-up value propositions of the EUDIWs towards citizens, pointing out concerns around use of data by private tech companies (Interviewee 18), design principles of the wallet to put individuals in control of their own data, (Interviewee 18), creating interactive demonstrations of wallet capabilities (Interviewee 18) Challenges may still persist to introduce citizens to the ecosystem where multiple digital identity offerings might be introduced and contextualized for citizen users, especially when principles of data sole control might be a new heuristic for citizens (Interviewee 18)

Similar to the service provider segment, technical implementation of the EUDIF has not been identified by public sector representatives as a significant barrier for organizational EUDIF adoption. (Interviewee 7) Instead, ecosystem governance and organizational-level change management have been identified as particular bottlenecks thereof. (Interviewee

7) They also recognize the importance of board or decision-maker support for successful EUDIF adoption (Interviewee 6). They recognize uncertainties, stemming from the regulatory developments in the ecosystem, as a barrier for new ecosystem players to assess risks and opportunities. (Interviewee 10) Moreover, exitance of political and top management support has been found critical for successful adoption (Interviewee 10) A representative underpins the importance of raising awareness in the ecosystem, describing benefits and value streams of the wallet to potential adopters (Interviewee 10) Representatives also voiced concerns for more transparency for ecosystem participants and data assets in the ecosystem to enable wallet use cases. (Interviewee 10; Interviewee 12) Similar to service providers, public sector representatives recognize wallet's data management propositions to be potentially incompatible with authentic source or registry business models. (Interviewee 10; Interviewee 21) Often, there are singular authentic sources of a given type of attribute; thus, the drive for innovation might be lower compared to relying parties, where one might find more motivation to innovate. (Interviewee 21) Compounded by the fact that their participation might be hampered by upfront investment requirements for compliance and technical readiness while a market with clear value propositions has not developed yet (Interviewee 10) Similar to service providers, a couple of suggestions have been posited to bridge this gap between current operations models and the needs of the credential sharing ecosystem. (Interviewee 10) Similar to service providers, public sector representatives also recognize the threat of a bare-minimum approach towards implementing the EUDIF (Interviewee 17), citing exclusive focus of governments to ensure compliance and deliver technical implementations, while not necessarily exclusive governance orchestration mechanisms to unlock value creation opportunities in the ecosystem. (Interviewee 17; Interviewee 21) On the individual level, representatives perceive that the existence of alternative and incumbent forms of digital identification may hamper EUDIW adoption. (Interviewee 14)

We were able to observe multiple public sector organizations in advanced stages of the EUDIW adoption process. We observe multiple instances of public sector organizations considering to be attribute issuers to wallets using internally owned or co-owned authentic data sources, in cooperation with private QTSPs and wallet providers (Interviewee 14; Interviewee 15) In such cases, a couple of business processes have already been internally considered to be transformed via EUDIW adoption. (Interviewee 14; Interviewee 18) The selection of such use cases depended on EUDIWs' implications on user privacy,

operational security of internal processes, and process efficiency for the public sector entity. (Interviewee 14; Interviewee 18) We were also able to observe representatives' familiarity with SSI concepts (Interviewee 14; Interviewee 18). Same representatives recognized the importance of communicating wallet-initiated changes in existing business processes and citizen journeys for transparency purposes (Interviewee 14). The driver behind this motivation is to reconcile citizens' trust in the public sector's adoption of the EUDIF. (Interviewee 14; Interviewee 18) In EUDIW practicing organizations, business-IT alignment gaps concerning EUDIF governance in internal ITG governance frameworks have been discovered. (Interviewee 14) Such ITG gaps are (1) complex procurement requirements, (2) lack of comprehensive requirements management capabilities, (3) lack of visibility on individual IT services and their value cases, and (4) lack of roadmap planning capabilities. (Interviewee 14) Moreover, from a process redesign perspective, designers might have to consider the EUDIWs as the new focal point of public digital service delivery. (Interviewee 18) Such changes may enable public sector organizations to rethink data requirements for different business processes and refactor them around wallet use cases to ramp up efficiency towards business processes. (Interviewee 18) To conclude our observations from the first evaluation round interviews. We generated our observations from 18 semi-structured stakeholder interviews in table format accessible in Annex C, where we grouped observations by level of analysis and identified barriers and drivers towards ecosystem participation and value creation assigned at every level, as well as the most commonly identified themes.

6.1.2 Presenting the first iteration of design objectives

Following our data analysis of the first evaluation round. We generated a final set of design objectives for an EUDIF governance model artifact The final set of design objectives presented below were initially derived from the corresponding literature which have been either concluded as supported by the initial round of evaluation interviews or they have been concluded as not supported and as a result will not be taken into account during design phases of the governance model artifact.

Evaluated design objectives	Design Objective	Supporting Interview(s)	Supporting Literature	Supported (Y/N)
1	Embed privacy-by-design capabilities in business processes	1, 7, 10, 12, 14, 17, 18, 25, 26	(Sedlmeir & Weigl, 2022), (Giannopoulou, 2023a)	Y
2	Support EUDIW use-case formulation	1, 2, 4, 5, 7, 8, 9, 10, 11, 13, 14, 18, 21, 22, 24, 26, 27	(Liesbrock & Sneiders, 2024), (Kolehmainen, 2021), (Laatikainen et al., 2025), (Degen & Teubner, 2024), (Weigl et al., 2023)	Y
3	Offer compliance management capability	4, 5, 7, 8, 9, 10, 14	(Laatikainen et al., 2025)	Y
4	Inform process redesign	3, 4, 5, 11, 12, 14, 18	(Laatikainen et al., 2025), (Kölbel et al., 2022)	Y
5	Support executive decision-making for EUDIF implementation	3, 4, 6, 7, 8, 9, 10, 11, 12, 14, 18, 21	(Liesbrock & Sneiders, 2024), (Kolehmainen, 2021), (Laatikainen et al., 2025), (Kölbel et al., 2022)	Y
6	Inform service design inputs	8, 9, 10, 14, 17, 18, 22, 26, 27	(Korir et al., 2022), (Liesbrock & Sneiders, 2024), (Korir et al., 2022), (Lockwood, 2021)	Y
7	Offer capability management functionality	5, 7, 8, 10, 12, 14, 15, 19		Y
8	Inform the technical implementation of digital identity solutions.	Not supported	(S. Lips et al., 2020) , (Mahula et al., 2024)	N

Table 2 Evaluated design objectives Author's elaboration

As a result of the evaluation process, we found that experts have not supported DO1. As previously discussed, most experts do not think that technical implementation governance of the EUDIF artifacts is particularly relevant to the problem space. Therefore, we have excluded DO1 from further consideration. Furthermore, during evaluation, we have uncovered a previously hidden design objective, DO7 on capability management functionalities, which has been voiced overwhelmingly by experts during evaluations. In total, we annulled a design objective while incorporating another one, keeping the total

number of design objectives the same between our literature review and first DSRM iteration cycle.

Furthermore, we present a separate set of high-level design objectives applicable to the governance model artifact. These requirements are defined as high-level and inherited requirements that pertain to the model's classification as a domain-specific, information technology governance model. In order to align with the generalized design objectives of such models, we present several high-level objectives that we have derived from the corresponding literature. These objectives are not subject to expert evaluations as they are directly inherited as an artifact trait.

High-level design objectives	Design Objectives	Supporting Literature
1	Depict organizational context in sufficient complexity.	(Wilkin & Chenhall, 2020)
2	Offer compatibility with common ITG frameworks in the public sector.	(Laita & Belaissaoui, 2017)
3	Offer compatibility with standard modelling tools and extensions.	(Laita & Belaissaoui, 2017)
4	Offer accountability capabilities.	(Wilkin & Chenhall, 2020), (Sroor et al., 2022)
5	Define relational structures and roles around the use of IT	(Wilkin & Chenhall, 2020), (Pool et al., 2018)

Table 3 High-level design objectives Author's elaboration

6.1.3 Demonstrating design objectives

Following (Peffers et al., 2007) we dedicate this section to demonstrating design objectives of the governance model in order to position our approach to problem solving in an organizational context. To this end, we lay out design considerations, approaches, and design concepts relevant to the seven identified design objectives of the model, considering the relevant literature before we present the construction stages of the governance model artifact. Some of the design objectives require discussion on our approach to operationalization of values in design considerations (DO1, DO2) while others require more context on our modelling approach (DO3, DO4, DO6, DO7) as a

result, we aim to ground our subsequent modelling approach towards domain-specific problem solving via this chapter's discussion.

DO1: Embed privacy-by-design capabilities in business processes

Considering the conceptual formulation of the EUDIW as a social value-bearing technical artifact. (European Commission, 2025) The organizational context of implementation and adoption cannot be thought separately from the values it aspires to introduce to the public sector organizational domain. (Sedlmeir & Weigl, 2022) In this context, the values of the wallet initiative, such as citizen privacy, data sovereignty, and data control (European Commission, 2025) Must be supported by concrete methods that can embed such values in organizational and technical ITG dimensions of a given public sector organization. Here, we recognize that values carried by the artifact must be a part of public sector business processes. (Giannopoulou, 2023b) and services (Korir et al., 2022) to have the desired effect in public service delivery. In the context of the first design objective of the governance model artifact, the concept of client privacy in government business processes comes into the spotlight.

> *"We are copying millions of identity data to thousands of organizations per year, such practices are not privacy friendly, so we would like to take advantage of the wallet in a more privacy preserving way. We would like it to be used to give citizens more control of their data but also give citizens the ability to share what is needed to make a transaction.." (Interviewee 7)*

Our pool of public sector representatives has confirmed the importance of utilizing EUDIW capabilities towards a more privacy-friendly and sovereign manner in public service delivery contexts. This may not only make them more efficient and secure but can also act as a reputation driver for the service offering institution. (Interviewee 24)

> *"..when we tried to explain what the EUDI Wallet is like, its principles like privacy by design, only you are in control of your own data that data is stored on your phone, some people don't belive it and some do believe it but they think it is going to be different because they don't trust the government.." (Interviewee 18)*

However, in practice, we observed a methodological gap to make such aspirations applicable in service delivery contexts. Without applying transparent methodologies, diversions in practice may occur; such diversions might otherwise lead to service

fragmentation or interoperability challenges. To address the methodological gap, we look towards the concept of selective disclosure as a cornerstone of EUDIW capability.

> *"..using the wallets can help in the sense that you can go into government workflows with attestations and controlling which attestations go where, wallets enable selective disclosure of attestations, and there is the value with data controllability.." (Interviewee 3)*

The ability of EUDIWs to selectively disclose identity attributes can enable more data control, lower operational and compliance costs in government processes, as fewer attributes will need to be stored. Selective Disclosure can also help enact increased privacy measures in processes through data minimisation, meaning that only specific data attributes required to complete a given process will need to be transmitted.

> *"..the opportunities are mostly in compliance, efficiency, time saving, cost saving, privacy preserving, autonomy, data minimisation but the way you organize the ecosystem will define the value of the risks which are on the other end of the scale. There are several opportunities, but the risk can weigh higher when you don't act upon the risks..(Interviewee 21)*

For our modelling approach, we ascertained that a possible methodological approach to embed increased client privacy and data control possibilities in public sector organizations is to propose a privacy-by-design framework to be used towards business process redesign. As a result, we have elected to use the privacy-by-design conceptual framework for process redesign by (van Rest et al., 2014a) and the data sovereignty conceptual model towards cross-border public services by (Da Silva Carvalho et al., 2023) The conceptual framework will be adopted as-is to be modeled, describing the main stages of privacy-by-design-driven process redesign in the public sector.

DO2: Support EUDIW use-case formulation

Use-case formulation in our thesis' context means a stage in organizational EUDIW adoption where strategic and managerial decisions are taken to determine wallet-adjacent value streams, revenue models, costs, and liabilities. Organizations also have to generate awareness about wallet technological capabilities and modes of value creation in the EUDIF ecosystem. This stage has been underpinned by experts as one of the most important controls to be proposed, as it may increase the likelihood of EUDIW organizational readiness (Interviewee 2; Interviewee 8) and positively affect EUDIW

adoption antecedents. (Interviewee 12; Interviewee 14) While a lack of use cases might affect such factors negatively. (Interviewee 15) This challenge is experienced more acutely in the government. (Weigl et al., 2023)

> *"..then you come to a difficult question which is going around for quite for some time, what is the actual business case and use case? People are still struggling and searching for the private sector to enable it and business use cases I see those questions popping up quite a lot in government the benefit is quite clear in the private sector in terms of what you can do. There is a quite bit of struggle of what the added value will be and the big question is who is going to pay for services, that is the biggest challenge in the sector I would say.." (Interviewee 8)*

Our approach to depicting such a process is to utilize our data to exhaustively identify activities, relations, and controls towards creating organizational use cases. We take into account technical capabilities, organizational and managerial context, and organizational value streams as the main adoption drivers. We recognize that value streams vary and differ for each public organization. Thus, we will model various decision-making stages in order to allow executive decisions to form the organizational use cases.

DO3: Offer compliance management capability

Compliance management is a critical aspect of our modelling approach. It has been demonstrated during expert interviews that compliance is a cornerstone requirement for any eIDAS adjacent transformation activity.

> *"..biggest mistake I see from government and private sector is that there is a project initiation, a certain scope and what they gather goals and budgeting but they tend to forget trust servcies operate in a very strict legal context and the big challenge is with digital transformation engagements is that they stat working from a technical point of view and more technical design and they try to see if that meets legal requirements and in most cases eIDAS framework is very narrow and very specific framework and you need to know the ins and outs of requirments to make a call on strategic transformation projects because once you start it is really challening to change requirements (Interviewee 8)*

Our approach to compliance management via modelling will be to incorporate certain design elements in an organizational context to inform technical and procedural constraints around process and service redesign. Our aim with our designed artifact is to identify compliance targets and inform organizations about which compliance

frameworks will be relevant for the EUDIF adoption context. We found that a higher-level approach towards compliance management is apt for our modelling context. Ultimately, compliance management capability will be handled as various inputs towards executive decision-making.

> *"..basically teaching governments and creating awareness of the legal framework on a higher level but making sure that a vision you have for a strategic alignment transformation does not substantially collide with any legal or regulatory requirements." (Interviewee 8)*

DO4: Inform process redesign

Business process change in the public sector was a recurring theme during our interviews. Knowledge gaps exist in the public sector about what implications adoption will bring, as well as controls and environments to manage such implications.

> *"..we need to rethink how to connect existing environments within the public sector, like systems and processes, to people who aim to make them easy, so you need some kind of centralized components.." (Interviewee 10)*

It is clear that process change around EUDIW adoption carries multiple dimensions, such that new capabilities introduced by the wallet can impact process redesign. There, awareness about EUDIW capabilities, organization capability, and motivation towards business process change are critical driving factors (Interviewee 11)

> *"..the biggest challenge here is with the migration from an analog process to a digital one, but you have to shape the whole process, so people have to rethink how they can really benefit from the new advantages of digitalization..".(Interviewee 11)*

Another dimension of EUDIW-driven process change is its potential to generate public value via transparent public service delivery. (Korir et al., 2022) However, it is critical that public sector organizations recognize value gaps in business processes. Identification of such gaps can be accelerated with a modelling approach to give administrators increased visibility over wallet capabilities and a structured approach towards EUDIW-driven business process redesign.

> *"..for the rental homes in the Netherlands, we have a process where there's a lot of discrimination. With the wallet, they can share only the income attribute.." (Interviewee 14)*

Process redesign has also been linked to the enactment of EUDIW principles in practical government tasks. Experts posit that EUDIW-driven process changes will have service-level effects that interface with the medium of public service delivery—underpinning the need for systematic scrutiny of change patterns in government processes as a result of wallet adoption.

> *"..we have to be focused on transparency, there are a lot of applications requesting personal data in the municipality context in the Netherlands, a lot of processes start with asking the citizen their ID number and with that number we get data from various systems to start service delivery, with the wallet processes will start with a presentation from the citizen wallet and that is quite a change for people.." (Interviewee 18)*

Our modelling approach towards this design objective is to identify necessary resources, organizational roles, and structures as preconditions to process redesign. Furthermore, we identify necessary process stages and considerations towards process redesign as organizations adopt wallets. Our goal with process redesign is to enable organizations to generate blueprint reference processes that can be reused for creating privacy-capable public service blueprints.

DO5: Support executive decision making for EUDIF implementation

Executive or management involvement in varying types of technology implementation contexts has been studied in theory and practice. (Baker, 2011) in the context of our thesis. Management support has been identified as crucial for successful EUDIW adoption. (Kölbel et al., 2022) Experts suggested that initiatives must consider not only executive contexts but should attempt to win the support of a diverse but highly relevant stakeholder body (Interviewee 10)

> *"..you need top management support to get the budget and resources to basically play with the wallet implementation, try to figure out what is the benefit and the value for them, and you need support from people who are responsible, for instance processes and products and they should be convninced that this helps them solve problems they have today.." (Interviewee 10)*

In our modelling approach, executive decision-making takes the center stage. We aim to use our data to connect organizational IT and process assets, as well as knowledge, to

executive oversight in order to enable the attainment of management involvement in the EUDIW adoption processes.

DO6: Inform service design inputs

Public services are one of the primary ways for citizen-government interactions. In our context, it is the medium for wallet-based citizen-government interactions. Scholars have identified design and user experience consistency in wallet-based services as detrimental to an individual's use and adoption of digital identity wallets. (Korir et al., 2022) Furthermore, as we strive to offer pathways for privacy-aware process redesign for wallet use cases, public services are the medium of their instantiations. (Interviewee 14) We can suggest that service design acts as a fundamental launchpad for the fulfillment of other objectives of our model in terms of ensuring that consistent, inclusive, wallet-aware, and technically and operationally capable service blueprints can be created in public sector organizations. Our focal point has been substantiated by experts as well.

> *"..if you would digitize the world around you in terms of wallet usage we would need to have a very consistent implementation in terms of how data is unlocked, presented and disseminated, if this process lacks coordination every service chain will digitize in their own way and that will result in inconsistencies, people will see the inconsistencies in the processes and they will question it, user acceptance is directly related to that.." (Interviewee 17)*

Our data suggests that service design considerations carry implications for EUDIWs' success. Service level considerations may not only elicit a more trustworthy wallet use environment, but they can also create auxiliary public value through the use of digital public services in a more transparent and trustworthy manner.

> *"..transparency is also important we tested with two different types of login buttons to our service portal one with the disclaimer that says you can chose which attributes to share and what worked out better, this also works as a design principle.." (Interviewee 18)*

Within this context, we formulate our modelling approach to service design as (1) enabling the generation of organizational awareness, such as collecting stakeholder needs and desires from wallet-based services, generating and updating IT and business requirements, and disseminating process and service ownership knowledge within the organization. We will also harness our data to propose specific controls, workflow stages, and activities to enable the creation of wallet-based service blueprints.

DO7: Offer capability management functionality

Organizational capabilities are a part of organizational governance assessments. (Chaffey, 2010) Our pool of experts considers organizational capabilities relevant to informing executive-level decision-making.

> *"..I think we will go towards a market where relying parties can contract an integrator which helps them speak to different wallets, this model needs to have the capability to know what is on the market and to decide if you have the capability in your own organization or are you outsourcing." (Interviewee 21)*

Specifically, one expert proposed the relevance of capability modelling practices to address governance challenges in the eIDAS ecosystem.

> *"..I would say that if we would have done more capability modelling up front then I think that would have been better, that would have led to a better alignment between these programs.." (Interviewee 19)*

We consider capability modelling and capability management as an integral component of our modelling approach. We aim to prescribe a sub-repository for organizational capability management. Similarly, we will construct management and operational level processes in compatibility with the institutional capability repository.

6.1.4 Selection of modelling tool, language, and framework

In this section, we will demonstrate our approach to selecting a suitable modelling tool and framework for the governance model artifact that fulfils high-level design objectives of such a governance model while allowing a satisfactory degree of compatibility with evaluated design objectives. During our data collection, we observed evidence of public sector organizations' use of ITG frameworks (Interviewee 14; Interviewee 15). Although the use of common frameworks like COBIT and ISO/IEC frameworks was present, interviewees suggested that they are customized and adapted to organizational contexts. (Interviewee 14; Interviewee 15) Furthermore, an interviewee found such frameworks too heavy to respond to the needs of an EUDIF adoption initiative and suggested agile governance frameworks as an alternative. (Interviewee 14) As a result, we structured our approach towards offering a customizable and adaptable model that fits the organizational ITG context as a domain-specific extension. To support the choice of a modelling framework, we offer multiple modelling frameworks and tools and offer a comparison

between their strengths and weaknesses, considering our use case. We considered (1) Scaled Agile Framework (SAFe), (2) Open Agile Architecture specification by the Open Group. (3) Disciplined Agile Framework. Although there is evidence of agile framework adoption in the public sector, specifically the use of the SAFe framework, agile frameworks need a certain degree of agile maturity in a given organizational context. (Conboy & Carroll, 2019) and has been found to require additional measures to be adopted. (Ciancarini et al., 2022) Another challenge with SAFe and the Disciplined Agile approach is the lack of reusable and modular components that can be used for domain-specific modelling projects. Furthermore, SAFe or Disciplined Agile do not incorporate a modelling language or a specific toolkit for customization. We found that the Open Agile Architecture specification (OAA) provides high-level reusable components, building blocks, and methods for depicting process-level and service-level alterations in organizations. Subsequently, we reviewed the OAA standard extensively to select relevant building blocks towards our modelling contexts. A list of 9 selected building blocks with corresponding modelling contexts has been generated and has been supplied in the thesis appendix in Annex J.

Considering the strengths and weaknesses of modelling frameworks, we have chosen to utilize Open Agile Architecture by the Open Group due to its extensive focus on government use cases, combining agile and traditional service delivery approaches for better contextual fit and its generalizable governance models toolkit, allowing modelers to configure and contextualize the model towards organizational settings. Moreover, OAA by the Open Group offers compatibility with widely practiced ITG governance frameworks as well as compatibility with further ITG artifacts such as capability models and enterprise architecture blueprints.

6.1.5 Demonstrating the governance model artifact

Following (Peffers et al., 2007) we constructed the first iteration of the governance model artifact. During construction, pre-selected building blocks from the OAA architecture specification were used for model wireframe construction. In total, we developed three main stages: (1) EUDIW use-case definition stage, (2) process redesign stage, and (3) service design stage using adapted OAA architecture elements. The model was constructed using Microsoft PowerPoint, which was then extracted from the program as a separate document. We provide the first iteration model as an intermediary artifact in

the research process; it has been attached to the appendix of this document and can be accessed in Annex K.

6.2 Design Science Cycle Second Iteration

Following (Peffers et al., 2007) we performed a second iteration of the DSRM cycle. The second iteration consists of holding 10 semi-structured interviews with subject-matter experts on the evaluation of the first iteration of the governance model artifact. First, we derived design-level changes after the analysis of the interview data. Secondly, the second and final iteration of the governance model artifact has been built. In this section, we will describe our second evaluation round, offer a detailed description of the governance model artifact in its second iteration, and finally, we will evaluate the design objectives at the final stage of the research to derive learnings from the modelling process.

6.2.1 Evaluating the governance model artifact

Subsequent to the completion of the first iteration of the model, we conducted 10 semi-structured expert interviews to evaluate the fit of the model to the given solution space. (Brocke et al., 2020) Our methodology for identifying interview partners, questionnaire design, and interview process was the same during the second round in order to ensure consistency in data collection. We supply the interview partners, their personal and organizational roles, as well as the durations of interviews, in a table in the appendix section of the thesis, accessible in the Annex E. In this sub-section, we will summarize our findings from the second evaluation round. Moreover, we will present multiple design change suggestions formulated as a result of our data analysis of the second round of interviews.

Firstly, evaluators suggested the relevance of ecosystem-level factors external to the adopting organization. (Interviewee 12) At the Member State level, organizations can disseminate knowledge about organizational data assets towards better ecosystem transparency. (Interviewee 12) On the organizational level, the relevance of business and IT requirements towards business process and service design changes has been pronounced. (Interviewee 14) Such requirements can also act as process and service constraint determinants (Interviewee 14). The Requirement management scope of the model can be extended to manage business and IT requirements from multiple, cross-functional teams that are collaborating. (Interviewee 14) Moreover, the model can be made to fit complex organizational contexts where business processes, capabilities, and

services are owned by different teams. (Interviewee 14) Similarly, service design stages should be able to accommodate the incorporation of varied stakeholder interests, concerns, and priorities. (Interviewee 14) Suggestions relating to model component hierarchies were made, such that three main depicted stages of EUDIF adoption may run in parallel (Interviewee 15; Interviewee 21)

Secondly, the relevance of broker and intermediary services for public sector EUDIF adoption has been underlined. (Interviewee 14; Interviewee 15; Interviewee 21) This aspect might necessitate a buy-build-reuse checkpoint stage in the use case definition stage of the model. (Interviewee 21) Further, participants identified relevant ecosystem-level components towards the use-case definition stage, such as availability of re-useable connectivity systems, technical components, and data models in Member States (Interviewee 15) and the political and administrative context in Member States. (Interviewee 15)

Following the conclusion of the secondary evaluation round, we formulated several design changes applicable to the initial form of the governance model. We generated a table of design changes of our elaboration and relevant design objectives, as well as supporting interviews. This table is accessible in the appendix of the thesis, situated in the Annex M.

6.2.2 Describing the governance model artifact

Following (Peffers et al., 2007) We will dedicate this section to describing, in detail, the features and capabilities incorporated in the presented artifact. We will also offer a description of prescribed workflows, facilities, structures, and control objectives resulting from organizational adoption of the model. We will explore the model in its six main stages in its final form in the context of this thesis. Continuing to the second evaluation round, three additional design elements were incorporated into the artifact, while contextual elements, workflows, and the organizational repository elements were kept as-is, as we have not received any corrections or requests for improvement. With the addition of three stages, we finalized our artifact for demonstration. The resulting artifact has been supplied in the appendix, accessible in Annex N.

6.2.2.1 Ecosystem context

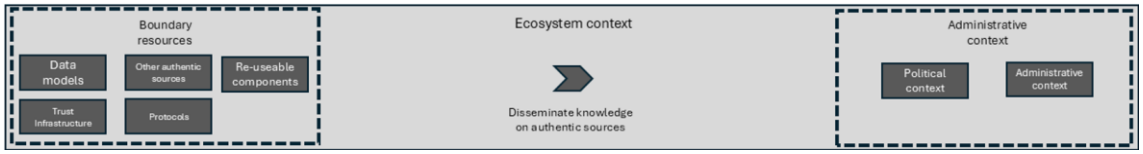

Figure 6 Ecosystem context Author's elaboration

Ecosystem context is a contextual element of the model that enables the execution of management functions towards relevant ecosystem activities that drive organizational participation in the EUDIF ecosystem. Use of this contextual element is therefore relevant for organizational decision-making. Within the element, we introduce two contextual blocks as boundary resources and administrative context. Towards the former block, ecosystem boundary resources are defined as common structures and resources that facilitate digital collaboration in an ecosystem setting. (Lukkien et al., 2023) The block can be consulted by implementing organizations to identify relevant ecosystem resources pertaining to EUDIF adoption. Furthermore, boundary resources are co-created between ecosystem participants. In the EUDIF context, baseline resources such as protocols and general trust infrastructures are defined by the Regulatory context (Interviewee 8) while data models (Interviewee 15) and re-useable components are often created at the Member State level. (Interviewee 9) In this stage, we recommend practitioners consider using this contextual block to identify and disseminate contextual information on organizational authentic sources, such as sample data models, if such an organization possesses ownership of authentic data sources. Sharing contextual data on custodial authentic sources may help increase transparency (Interviewee 12) of Member State EUDIF implementation governance mechanisms and enable other participants to develop wallet use cases based on the reuse of authentic data. (Interviewee 10)

The latter part of the element presents administrative and political contextual blocks. These are relevant for practitioners to consider the political and administrative contexts within a Member State. States exhibiting a strong multi-level governance tradition can result in higher degrees of implementation purview at the cost of an increase in implementation costs and efforts. (Interviewee 7; Interviewee 15) Similarly, the availability of boundary resources may vary depending on the political support behind implementation efforts. (Interviewee 17) Other governmental organizations acting as ecosystem orchestrators can make available or constrain the availability of boundary

resources. Hence, monitoring of the political and administrative landscape is recommended for implementation practitioners to not only ensure the success of specific digital transformation projects but also to ensure the sustainability and scope fulfillment.

6.2.2.2 Organizational governance context

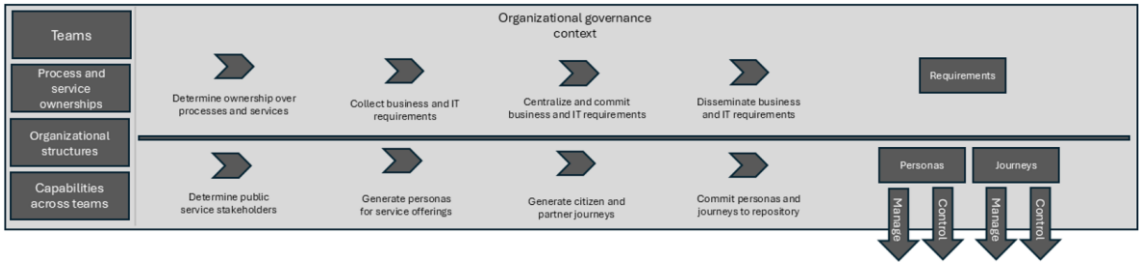

Figure 7 Organizational governance context Author's elaboration

Organization governance is another contextual block introduced for the internal management of activity stages. Public sector representatives demonstrated the relevance of centralized requirements management (Interviewee 14; Interviewee 6), especially for large organizations where multiple teams can collaborate concerning a digital identity adoption project. (Interviewee 14) We propose that organizations identify relevant teams and their process and service responsibilities before executing the first workflow. Subsequently, business and IT requirements towards service and process level changes can be collected across teams and business units by regular panel meetings. The resulting requirements should be committed to the organizational repository block for further reuse and reference. Furthermore, we suggest that organizations disseminate such information to their external stakeholders as requirements form the basis for contractual relationships with EUDIF component suppliers. We propose this step to enable a more streamlined procurement process for both sides, as unclear or non-harmonized requirement practices have been reported by service providers previously. (Interviewee 6)

The latter part of the block has been modelled to enable the customization of EUDIW-based public service offerings. Such services can have many different stakeholders, including but not limited to locally domiciled individuals (Interviewee 18), nationally domiciled individuals (Interviewee 15), cross-border users (Interviewee 14), as well as locally, nationally, or European-wide incorporated businesses. (Interviewee 2) As a result, we model several workflow stages, proposing the use of citizen and user personas (Interviewee 14) and citizen journeys (Interviewee 14; Interviewee 18), which can allow

service designers to centralize service-level design objectives' management while also permitting an ample level of variety for consideration towards service design. Citizen journeys might offer the creation of stop-gap solutions on top of existing public service blueprints (Interviewee 28), removing the need for designing blank slate solutions to allow for graceful transitions (Interviewee 11) and aid the creation of more inclusive service blueprints when used in tandem with user personas. (Interviewee 26) We recommend that formulated citizen journeys and personas be committed to the organizational repository for continuous feedback, improvement, and management reference throughout the implementation process.

6.2.2.3 Use case formulation stage

Figure 8 Use case formulation stage Author's elaboration

Use case formulation is a stage element, modelled to refrain from commonly identified pitfalls of EUDIW adoption. Experts unanimously agree on the importance of clear, well-operationalized organizational use cases for wallet adoption. Hence, this stage fulfils the purpose of defining the contexts and processes where EUDIW adoption can be beneficial. We recommend that implementors consider the existing best practices and use cases already in demonstration in the ecosystem, and consider demonstrated motivations of their key stakeholders towards using digital identity wallets. Subsequently, the initiated workflow takes organizational use motivations into account to create a suitability assessment considering compliance requirements related to EUDIW adoption. During this process, the organizational repository's compliance sub-element can be consulted, and newly identified requirements can be committed to the repository. Suitability assessments conclude with the identification of existing organizational data and IT assets. (Interview 14) Availability of authentic or authoritative sources in organizational custody may have an impact on use cases, determining the participation modes of a given organization as a potential authentic or authoritative data provider. In such cases, further management actions might be necessary to plan for and to conclude contracts with (Q)TSPs. Organizations should formulate high-value, priority interventions, taking into account EUDIW technical capabilities, identified data and IT assets, and use motivators

and compliance requirements. We define high-value interventions as pragmatic and practical considerations that prioritize the use of EUDIWs in high-utilization and high-demand use cases. Experts previously agreed that such interventions are likely to be around automatic identity and attribute verification, secure authentication, and data sharing use cases. Thus, we recommend that practitioners consult existing use cases, pilot projects, and best practices before determining high-value interventions in their organizations. Finally, we recommend a buy-build-reuse decision to be taken during the use-case definition stage (Interviewee 21; Interviewee 15) relating to identified data and IT assets. We observed that complexities attached to meeting compliance requirements (Interviewee 8) and lack of organizational resources (Interviewee 15) can drive public sector organizations to reusing ready technical components or buying it from service providers in the form of digital identity broker middleware, (Interviewee 25) off-the-shelf identity and access management components (Interviewee 14) and wallet solutions. (Interviewee 22) Considering such constraints, we recommend implementers finalize use case definition rounds with a buy-build-reuse decision that takes the desired scope of EUDIW adoption, goals of the wallet-adoption project, and resources that have been made available for the wallet adoption. The result of this decision can introduce contractual dependencies and obligations towards component providers and trust service providers that can translate into further project costs.

6.2.2.4 Process redesign stage

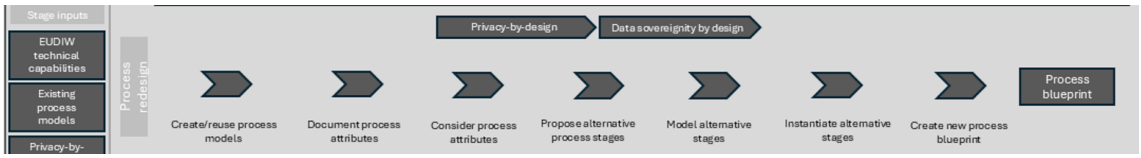

Figure 9 Process redesign stage Author's elaboration

Process redesign is a stage element defining a workflow that proposes an operational approach towards privacy-by-design and data-sovereignty-by-design principles in public sector business processes. Earlier, we found that EUDIF's ecosystem formulation as presented in the ARF incorporates similar ecosystem goals and design principles (European Commission, 2025) Experts have underlined the relevance of process redesign around the new capabilities of EUDIWs (Interviewee 4; Interviewee 14) We recommend implementors to consider existing process models and novel technical capabilities offered

by EUDIWs such as selective disclosure towards business processes. In the workflow model, we depict the main stages of process redesign embedded in privacy-by-design and data-sovereignty-by-design principles, previously conceptualized and presented by.(Da Silva Carvalho et al., 2023) and (van Rest et al., 2014a). In their conceptual model, we found the scholarly conceptual context meaningful as it provides a practical method for informing organizational process redesign for affording public service clients increased control over their data, privacy, and sovereignty of their data attributes. We recommend that implementers consider the mandatory and optional attributes collected at each stage of existing model processes, propose an alternative process stage that incorporates fewer data attributes while still achieving the same process goal. We found that wallet-based processes can be utilized to combat biases using selective disclosure of identity attributes. (Interviewee 14; Interviewee 18), At the same time, existing instances of such processes may result in the reproduction of similar biased outcomes. In that sense, we maintain the position that organizations should pay attention to novel wallet capabilities, document such capabilities, and refer to them while considering whether similar process enhancements are done. Afterwards, alternative process stages should be modelled using proper BPM techniques and practices. We recommend that organizations instantiate processes before committing them to process blueprints to ensure that unwanted deviations in the public service delivery do not occur. (Interviewee 17) After instantiation, the process blueprint will be created as an input towards the organizational process repositories and for the next design stage.

6.2.2.5 Service design stage

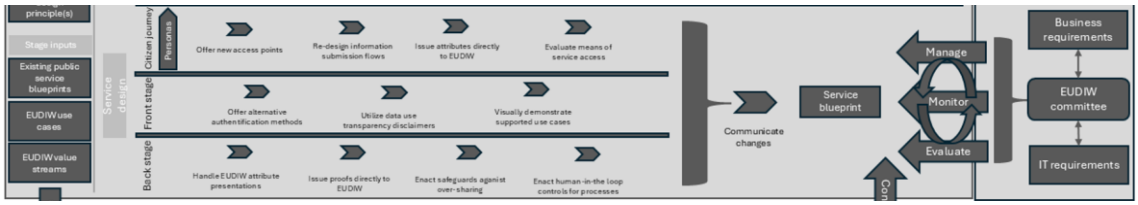

Figure 10 Service design stage Author's elaboration

Service design is the last stage element in the governance model. This stage incorporates a three-story workflow design where we modelled controls, activities, and constraints for EUDIW-based service design. Further, we model the essential role of the EUDIW committee as the main steering body, governing the organizational EUDIW adoption processes. Service design is another important aspect of complete EUDIF adoption in

public sector organizations. Experts identified the need for consistency (Interviewee 17), inclusivity (Interviewee 26), proactiveness (Interviewee 14), and citizen-centric design (Interviewee 18) towards service design. Use of EUDIWs can also create entirely new digital or physical interfaces for public service delivery (Interviewee 28), requiring changes in service access, delivery, and termination mediums. In this stage, we modelled a three-stage representation of a service delivery workflow, incorporating client-facing activities, front-stage activities consisting of digital or physically executed activities that are directly visible to public service clients, and backstage activities related to the digital back-end operations or back-office actions in case of physical service execution. We recommend that implementors take into account previously defined EUDIW use cases and process blueprints as inputs towards service design. We also stress that service design is an iterative process similar to the process design stage of the model. Thus, we recommend that practitioners consult already existing manuals and service models and use our stage model for identifying suitable improvements. We identify offering new access points (Interviewee 28), re-designing information submission interfaces (Interviewee 18), issuing attributes to digital identity wallets (Interviewee 1), and continuous evaluation of service access interfaces (Interviewee 28) as design considerations for transforming existing citizen journeys. Moreover, service designers may consider offering alternative authentication methods along with digital identity wallets for increased service inclusion (Interviewee 25). They can also embed data use transparency disclaimers (Interviewee 18) and enact demonstrations of citizen wallet use cases in service delivery points. (Interviewee 18) Technologically, services should be capable of handling EUDIW attribute presentations and subsequent processing of presented attributes. For greater transparency, we recommend enacting institutional safeguard processes against intentional or accidental over-sharing by citizen wallets. Over-sharing may occur when clients present attributes via their wallets in unnecessary verbosity. (Interviewee 25) While experts suggest that native safeguards against over-sharing might exist within EUDIWs. We recommend setting attribute constraints for given service design and process design blueprints in order to combat the challenges of over-sharing. A service design blueprint finalizes with the communication of service-level design changes. At this stage, we recommend that organizations determine the relevance of wallet-based services for other ecosystem actors. For example, other public sector entities or private businesses can act as relying parties towards a wallet-based service. In such instances, collaborative value creation mechanisms at the ecosystem level

can be explored further by clarifying service offerings for citizens, businesses, regional, local, and national governmental entities. Service blueprints are the primary outputs of our governance model, incorporating the use case and process blueprint inputs from preceding stages. Service blueprints are managed, monitored, and continuously evaluated by the EUDIW committee. EUDIW committee assumes the role of organizational orchestrator.

6.2.2.6 Organizational repository context

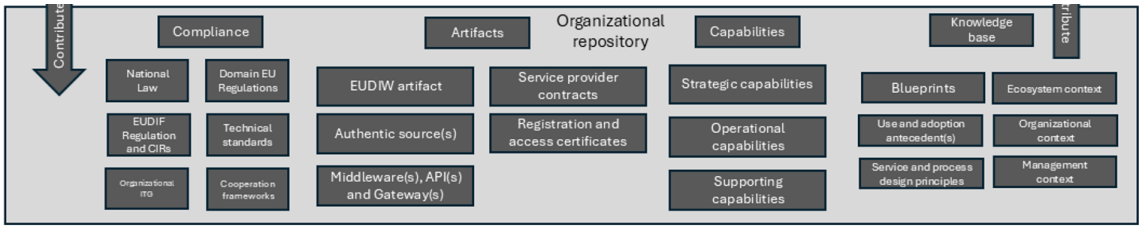

Figure 11 Organizational repository context Author's elaboration

The organizational repository is the final contextual element of the model. It consists of compliance, artifact, capabilities, and knowledge base sub-elements. The repository acts as the centralized base storage of requirements, controls, and models that have been generated as a result of the execution of other stages or contextual elements. Experts identify compliance management as a critical activity for any organization implementing a wallet. (Interviewee 8) Comprehensive compliance management should consider the EUDIF as well as national laws, domain regulations, and directives in the European Union, such as the Cyber Resilience Act (CRA), the NIS2 Directive, and the General Data Protection Regulation (GDPR). Public sector organizations developing or contracting technical solutions should assess their compliance with harmonized technical standards. (Interviewee 8) The repository records the custodial artifacts that organizations can acquire and manage during EUDIF adoption. Primarily, organizations can possess two types of wallet relations: wallet operators or wallet relying parties. A public sector organization can possess ownership over authentic sources of citizen, business, or entity identifiers, or it can act as a relying party to such data points. Organizations can operate connectivity middleware solutions, identity broker intermediaries that facilitate connectivity between recognized wallets and organizational IT assets, relying party registration certificates, relying party access certificates, or contract their provision and operation to third parties. Organizational capabilities have also been incorporated in the

repository as they have been identified by experts as relevant. (Interviewee 19) We recognize capability management as a business unit-specific function under the governance of the EUDIW committee role in order to offer a centralized overview of acquired and maintained capabilities. Finally, the knowledge base element represents factual organizational and peripheral data, incorporating stakeholder attitudes about EUDIW adoption and committed service and process blueprints.

6.2.3 Evaluating the design objectives of the governance model artifact

Following (Peffers et al., 2007) We conclude our results with a demonstration of the final stage of design objectives. We will offer an overview of achieved artifact traits and discuss goal achievement metrics and the extent to which our artifact has achieved desired success objectives. In order to present a set of objectives for evaluation, we use the framework for identifying research objectives in DSRM. (Alismail et al., 2017) The framework suggests that DSR objectives shall carry a set of success criteria, including descriptions of problem level and stakeholders, level of goal achievement, and achieved artifact traits.

Design objective		Success Requirements		
		Problem Level & Stakeholders	**Goal Achievement**	**Artifact Trait**
1	Embed privacy-by-design capabilities in business processes	Organizations, individuals	Partial attainment	Offers incorporation of PbD in process redesign
2	Support EUDIW use-case formulation	Organizations	Fully supported	Offers specialized use-case formulation stage
3	Offer compliance management capability	Organizations	Fully supported	Identifies compliance targets
4	Inform process redesign	Organizations	Fully supported	Offers specialized process redesign stage
5	Support executive decision-making for EUDIF implementation	Organizations, EUDIF ecosystem participants	Fully supported	Identifies organizational controls, proposes repositories, and hierarchies towards EUDIF governance
6	Inform service design inputs	Organizations, individuals	Fully supported	Offers specialized service design stage
7	Offer capability management functionality	Organizations	Partial attainment	Connect organizational capabilities to EUDIF adoption

Table 4 Evaluating the design objectives of the governance model artifact Author's elaboration

We can report that our artifact exhibits traits to fully support 5 out of 7 design objectives, while partially supporting two design objectives. We found that DO1 has been only partially supported as our operationalization of Privacy-by-design principles (PbD) extended as far as process lifecycles, while PbD applications suggest a whole of the data lifecycle approach. (van Rest et al., 2014b) However, incorporating data attribute lifecycles in their entirety has not been found within the scope of this thesis. Moreover, DO7 has also been partially supported as our model does not identify and propose specific organizational capabilities for governing EUDIF adoption besides prescribing a relational hierarchy and a management function attached to their identification. We suggest that achieving full attainment of the seventh design objective requires an auxiliary capability model artifact that carries a separate set of design objectives and application context. At the same time, our modelling approach has been structured to allow for model extensions and integration of existing capability models. As a result, organizations can still utilize the governance model by supplying the organizational repository with existing capabilities and executing the management actions that result in their continuous use.

Furthermore, we present our evaluation of the high-level inherited artifact traits from a modelling point of view in the table in Annex Q. We found that our governance model artifact may fully support 3 out of 5 high-level design objectives. We observe that, among high-level design objectives, DO1 might require context-specific customization of the artifact to reach a fully supported status, as organizational governance contexts might differ on a case-by-case basis. Moreover, we found partial support for DO4 as we did not have the scope to scrutinize ITG model accountability mechanisms for our modelling approach.

7 Discussion

In this section, we discuss the implications of our findings for the digital identity wallets research domain. We will also discuss the implications of the use of our governance model in public sector organizations. Afterwards, we discuss various limitations of our thesis from methodological and research resources perspectives. We will conclude this section with our recommendations for further research perspectives based on the knowledge gaps we were able to survey during our research process.

Firstly, we are able to confirm the findings of multiple scholarly articles. Within our findings, we observe the importance of the government orchestration function for collaborative value creation in the EUDIF ecosystem. We can confirm the need for consideration of public and private business models and ecosystem tensions for the successful implementation of EUDIF prerogatives. (Degen & Teubner, 2024) We were able to observe, in significant overlap, very similar barriers for EUDIW development. (Lukkien et al., 2023) Thus, we can confirm the accuracy of the barrier classification scheme introduced by the authors. We observed the challenge of oversharing attached to EUDIW use in practice, as suggested by (Marsman et al., 2024)

Secondly, as we were able to confirm the suitability of design objectives through rigorous analysis, we can suggest that the use of our governance model artifact may carry implications for organizational EUDIF adoption governance in the public sector. We suggest that our model can enable baseline privacy-by-design capabilities in EUDIW, adopting public sector organizations by informing process redesign towards data-minimising disclosure and information submission practices. Organizations that enact such process changes may be able to incorporate the design principles of the EUDIWs in business processes, foster stakeholder trust through process-client privacy. Furthermore, the use of our model can prevent common pitfalls of information technology enactment. Organizations can utilize our model to identify wallet-enabled value streams, priority use cases, and collaborative value creation mechanisms, thus creating conditions for sustainable and performant use of EUDIWs in organizational contexts. Furthermore, our model can be utilized towards compliance management activities, as we propose organizational roles and relational entity hierarchies for compliance activities. Organizations might elect to use it to contextualize different angles of compliance activities towards service and process blueprints.

In sum, with the use of our artifact, organizations can avoid common pitfalls of EUDIW adoption, namely IT underuse and business-IT non-alignment scenarios. We recognize, in our modelling approach, that value creation in the EUDIF ecosystem is inherently collaborative. As such, we propose comprehensive ecosystem activities, controls, and functions towards contributing to ecosystem-level collaborative value creation activities, organizational-level governance workflows in order to centrally manage process and service requirements as well as stakeholder journeys. We offer controls, constraints, and activities for organisations to transform existing process and service blueprints towards EUDIW-native offerings via the incorporation of EUDIF ecosystem principles and goals. We expect that with the adaptation of our governance model, given that it has been customized and harmonized with organizational implementation context and existing ITG controls, organizations can unlock the pre-conditions for organizational service-level value creation towards immediate stakeholders and ecosystem-level collaborative value creation in the EUDIF ecosystem. We aspire that the adoption of our artifact may enable public sector organizations to participate, collaborate, and innovate with data sharing solutions towards a more secure, inclusive, innovative, and forward-looking digital identity ecosystem in the European Union.

7.1 Limitations

Throughout the thesis, we aimed to attain generalizability for our proposed governance model by surveying a diverse and adjacent literature, ensuring that all relevant EUDIF ecosystem stakeholders from multiple European Union Member States are represented in our expert interviews and utilizing relevant modelling frameworks appropriate for the given context. We utilized a finalized version of the EUDIF Regulation and an up-to-date version of ARF that posits enough conceptual complexity and EU-level harmony to enable generalizability for our purposes. Subsequently, we integrated design and use principles of EUDIWs enumerated in the EUDIF Regulation, which will be implemented uniformly across Member States. However, we recognize that our thesis is limited in various ways. Firstly, the EUDIF Regulation as well as the ARF are being actively implemented with several Commission Implementing Regulations (CIRs) still due for adoption. The fast pace of regulatory developments at the EU and Member State levels may necessitate reconsiderations, updates, and adaptations of the model. Secondly, due to the current stage of the EUDIF implementation, it was not feasible to observe organizational contexts where EUDIWs have been actively used or implemented. Hence,

limiting our empirical lens on practical challenges, drivers, and barriers. Thirdly, due to time constraints, we have not been able to employ a longitudinal lens on organizational EUDIW adoption, which would have afforded our research extra capabilities to demonstrate the process of wallet adoption, wallet-driven value creation, and wallet-driven organizational digital transformation. Fourth, our pool of experts almost exclusively represents Northern and Central European countries. As a result, our design objectives and resulting governance model cannot claim pan-European applicability. Fifth, our thesis did not consider national laws and regulations around data protection, sharing, and use, which carry implications for the customization of EUDIF governance models in implementation. Lastly, our perspective of the EUDIF ecosystem playing field, actor roles, and governance tensions was shaped by the available literature and ecosystem-level insights obtained via semi-structured interviews. Hence, we cannot claim universal exhaustiveness of institutional governance factors applicable to a given European public sector institution. For that, we aimed to construct our governance model artifact as flexibly, high-level, and customizable as possible.

7.2 Further research perspectives

In order to bridge several gaps we have observed during this study, we recommend further research scrutinizing the EUDIF trust framework's assumptions and offerings from an organizational perspective to offer a deeper understanding of organizational digitally mediated trust in the public sector. Focusing on actor perspectives towards EUDIF ecosystem participation, incentives, drivers, and barriers for EUDIF adoption. Demonstrating governance aspects of organizational EUDIW success in other EU regions. Presenting requirements, challenges, and pathways for EUDIF governance models from a national law and regulatory perspective, and demonstrating governance implications of EUDIF from a pan-European ecosystem perspective that scrutinizes the role of the private sector players and specialized governance bodies in Member States. We recognize that as the deadlines for implementation draw closer, knowledge on the practical implications of EUDIF governance in the public sector will become more valuable.

8 Conclusion

The adoption of the European Digital Identity Framework Regulation in 2024 has introduced implementation deadlines for European public sector organizations to adopt European Digital Identity Wallet use cases. However, simple implementation measures may hinder the exploitation of the true extent of value creation opportunities in the digital platform ecosystem that is being introduced by the Regulation. We employ a Design Science Research lens towards analysing the governance of value creation mechanisms in a novel digital platform ecosystem. To this end, we propose an intra-organizational governance model artifact for public sector organizations to govern value creation mechanisms via European Digital Identity ecosystem participation and through the adoption of European Digital Identity Wallets. Our artifact has been designed through the application of the DSRM cycle, incorporating two evaluation rounds of semi-structured interviews attended by 28 subject-matter experts from ecosystem organizations. We found that our artifact fully supports 5 out of 7 design objectives while exhibiting the ability to support two additional objectives. Within a modelling context, we identify modes and methods of creating singular and collaborative value through the use of digital identity wallets in the public sector, and we identify organizational roles, relational structures, hierarchies, controls, constraints, and knowledge bases towards a value-informed governance of the European Digital Identity Wallets in the public sector. Our findings may allow researchers and practitioners of European Digital Identity to derive practical governance learnings and help inform the digital identity wallet governance practice in European public sector organizations.

References

Addo, A. (2022). Orchestrating a digital platform ecosystem to address societal challenges: A robust action perspective. *Journal of Information Technology*, *37*(4), 359–386. https://doi.org/10.1177/02683962221088333

Alhassan, I., Sammon, D., Daly, M., Wibisono, A., Kasraian, L., Nagle, T., Heavin, C., Dennehy, D., Zamani, E., & Qaffas, A. (2023). THE USE OF OPEN, AXIAL AND SELECTIVE CODING TECHNIQUES: A LITERATURE ANALYSIS OF IS RESEARCH. *UK Academy for Information Systems Conference Proceedings 2023*. https://aisel.aisnet.org/ukais2023/20

Alismail, S., Zhang, H., & Chatterjee, S. (2017). A Framework for Identifying Design Science Research Objectives for Building and Evaluating IT Artifacts. *Designing the Digital Transformation*, 218–230. https://doi.org/10.1007/978-3-319-59144-5_13

Ammann, J., & Hess, T. (2025). To sell, to donate, or to barter? Value creation and capture through business model types in decentralized data ecosystems. *Electronic Markets*, *35*(1), 1–22. https://doi.org/10.1007/s12525-025-00775-x

Autio, E. (2022). Orchestrating ecosystems: A multi-layered framework. *Innovation*, *24*(1), 96–109. https://doi.org/10.1080/14479338.2021.1919120

Baker, J. (2011). *The Technology–Organization–Environment Framework*. ResearchGate. https://www.researchgate.net/publication/226145805_The_Technology-Organization-Environment_Framework

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386. https://doi.org/10.2307/248684

Benbasat, I., & Zmud, R. W. (1999). Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly*, *23*(1), 3–16. https://doi.org/10.2307/249403

Bender, B., & Heine, M. (2021). Government as a Platform? Constitutive Elements of Public Service Platforms. *Electronic Government and the Information Systems Perspective*, 3–20. https://doi.org/10.1007/978-3-030-86611-2_1

Berghout, E., & Tan, C.-W. (2013). Understanding the impact of business cases on IT investment decisions: An analysis of municipal e-government projects. *Information & Management*, *50*(7), 489–506. https://doi.org/10.1016/j.im.2013.07.010

Bharosa, N., Lips, S., & Draheim, D. (2020). Making e-Government Work: Learning from the Netherlands and Estonia. *Electronic Participation*, 41–53. https://doi.org/10.1007/978-3-030-58141-1_4

Bochnia, R., Richter, D., & Anke, J. (2024). Self-Sovereign Identity for Organizations: Requirements for Enterprise Software. *IEEE Access*, *12*, 7637–7660. https://doi.org/10.1109/ACCESS.2023.3349095

Bodó, B. (2021). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*, *23*(9), 2668–2690. https://doi.org/10.1177/1461444820939922

Brocke, J. vom, Hevner, A., & Maedche, A. (2020). *Introduction to Design Science Research* (pp. 1–13). https://doi.org/10.1007/978-3-030-46781-4_1

Cap, C. H., & Maibaum, N. (2001). Digital Identity and its Implication for Electronic Government. In *Towards the E-Society* (pp. 803–816). Springer, Boston, MA. https://doi.org/10.1007/0-306-47009-8_59

Chaffey, D. (2010). Applying organisational capability models to assess the maturity of digital-marketing governance. *Journal of Marketing Management*, *26*(3–4), 187–196. https://doi.org/10.1080/02672571003612192

Chang, S.-I., Yen, D. C., Chang, I.-C., & Jan, D. (2014). Internal control framework for a compliant ERP system. *Information & Management*, *51*(2), 187–205. https://doi.org/10.1016/j.im.2013.11.002

Cheesman, M. (2022). Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. *Geopolitics*, *27*(1), 134–159. https://doi.org/10.1080/14650045.2020.1823836

Ciancarini, P., Kruglov, A., Pedrycz, W., Salikhov, D., & Succi, G. (2022). Issues in the adoption of the scaled agile framework. *Proceedings of the 44th International Conference on Software Engineering: Software Engineering in Practice*, 175–184. https://doi.org/10.1145/3510457.3513028

Conboy, K., & Carroll, N. (2019). Implementing Large-Scale Agile Frameworks: Challenges and Recommendations. *IEEE Software*, *36*(2), 44–50. https://doi.org/10.1109/MS.2018.2884865

Corbin, J., & Strauss, A. (2014). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications.

Da Silva Carvalho, N., Jabbarpour, J., Temple, L., Belacort, I. M., Barturen, U. I., Kortlander, M., Sanchez Pelaez, V., Areizaga Sanchez, E., & Mureddu, F. (2023). A more inclusive Europe through personal data sovereignty in cross-border digital public services. *Proceedings of the 16th International Conference on Theory and Practice of Electronic Governance*, 63–71. https://doi.org/10.1145/3614321.3614329

de Mildt, M., Verbrugge, S., & Colle, D. (2025). A market analysis on data ecosystem initiators and their value propositions in different ecosystems. *Telecommunications Policy*, *49*(3), 102910. https://doi.org/10.1016/j.telpol.2025.102910

Debreceny, R. S. (2013). Research on IT Governance, Risk, and Value: Challenges and Opportunities. *Journal of Information Systems*, *27*(1), 129–135. https://doi.org/10.2308/isys-10339

Debreceny, R. S., & Gray, G. L. (2013). IT Governance and Process Maturity: A Multinational Field Study. *Journal of Information Systems*, *27*(1), 157–188. https://doi.org/10.2308/isys-50418

Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets*, *34*(1), 50. https://doi.org/10.1007/s12525-024-00731-1

European Commission. (1999). *Directive 1999/93*. https://eur-lex.europa.eu/eli/dir/1999/93/oj/eng

European Commission. (2014). *Regulation—910/2014—EN - e-IDAS - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

European Commission. (2022). *2030 digital decade policy programme | EUR-Lex*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4646000

European Commission. (2024). *Regulation 2024/1183*. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

European Commission. (2025). *Architecture and Reference Framework*. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access*, *7*, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173

Foundation, T. over I. (2021). *GSWG Glossary*. https://trustoverip.github.io/gswg/glossary#trust-community

Giannopoulou, A. (2023a). Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity. *Digital Society*, *2*(2), 1–19. https://doi.org/10.1007/s44206-023-00049-z

Giannopoulou, A. (2023b). Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity. *Digital Society*, *2*(2), 1–19. https://doi.org/10.1007/s44206-023-00049-z

Giannopoulou (Alexandra), & Wang (Fennie). (2021, April 20). *Self-sovereign identity* [Info:eu-repo/semantics/article]. Alexander von Humboldt Institute for Internet and Society gGmbH. https://doi.org/10.14763/2021.2.1550

Göran, G. (2019). The Generation of Qualitative Data in Information Systems Research: The Diversity of Empirical Research Methods. *Communications of the Association for Information Systems*, 572–599. https://doi.org/10.17705/1CAIS.04428

Granstrand, O., & Holgersson, M. (2020). Innovation ecosystems: A conceptual review and a new definition. *Technovation*, *90–91*, 102098. https://doi.org/10.1016/j.technovation.2019.102098

Group, O. (2025). *The O-AA™ Standard | www.opengroup.org*. https://www.opengroup.org/AgileArchitecture

Günther, W. A., Mehrizi, M. H. R., Huysman, M., & Feldberg, F. (2017). *Debating big data: A literature review on realizing value from big data—ScienceDirect*. https://www-sciencedirect-com.kuleuven.e-bronnen.be/science/article/pii/S0963868717302615?via%3Dihub

Gupta, B., Dasgupta, S., & Gupta, A. (2008). *Adoption of ICT in a government organization in a developing country: An empirical study—ScienceDirect*. https://www-sciencedirect-com.kuleuven.e-bronnen.be/science/article/pii/S0963868707000650?via%3Dihub

Hagiu, A., & Wright, J. (2015). Multi-sided platforms. *International Journal of Industrial Organization*, *43*, 162–174. https://doi.org/10.1016/j.ijindorg.2015.03.003

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. *Electronic Markets*, *30*(1), 87–98. https://doi.org/10.1007/s12525-019-00377-4

Herz, T. Ph., Hamel, F., Uebernickel, F., & Brenner, W. (2013). Toward a model of effective monitoring of IT application development and maintenance suppliers in multisourced environments. *International Journal of Accounting Information Systems*, *14*(3), 235–253. https://doi.org/10.1016/j.accinf.2012.12.003

Hevner, A., vom Brocke, J., Winter, R., & Maedche, A. (2020). *Accumulation and Evolution of Design Knowledge in Design Science Research—A Journey Through Time and Space*. ResearchGate. https://www.researchgate.net/publication/336568065_Accumulation_and_Evolution_of_Design_Knowledge_in_Design_Science_Research_-_A_Journey_Through_Time_and_Space

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The Relationship between Board-Level Technology Committees and Reported Security Breaches. *Journal of Information Systems*, *30*(3), 79–98. https://doi.org/10.2308/isys-51402

Hölbl, M., Kežmah, B., & Kompara, M. (2023). eIDAS Interoperability and Cross-Border Compliance Issues. *Mathematics*, *11*(2), Article 2. https://doi.org/10.3390/math11020430

Institute, I. G. (2003). *Board Briefing for IT Governance, 2nd Edition*. Information Systems Audit and Control Association.

Ishmaev, G. (2021). Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and Information Technology*, *23*(3), 239–252. https://doi.org/10.1007/s10676-020-09563-x

Jewer, J., & McKay, K. N. (2012). *"Antecedents and Consequences of Board IT Governance: Institutional and" by Jennifer Jewer and Kenneth N. McKay*. https://aisel-aisnet-org.kuleuven.e-bronnen.be/jais/vol13/iss7/1/

Karhade, P., Shaw, M. J., & Subramanyam, R. (2015). *"Patterns in IS Portfolio Prioritization" by Prasanna Karhade, Michael J. Shaw et al.* https://aisel-aisnet-org.kuleuven.e-bronnen.be/misq/vol39/iss2/9/

Kernstock, P., Altenkamp, P., Böttcher, T., Hein, A., & Krcmar, H. (2025). *A Configurational Approach to Understanding Data Ecosystems*. https://hdl.handle.net/10125/109326

Kim, G., Shin, B., Kim, K. K., & Lee, H. G. (2011). *"IT Capabilities, Process-Oriented Dynamic Capabilities, and Firm Finan" by Gimun Kim, Bongsik Shin et al.* https://aisel.aisnet.org/jais/vol12/iss7/1/

Kohli, R., & Johnson, S. (2011). (PDF) Digital transformation in latecomer industries: CIO and CEO leadership lessons from Encana Oil & Gas (USA) Inc. *ResearchGate*. https://www.researchgate.net/publication/220500653_Digital_transformation_in_latecomer_industries_CIO_and_CEO_leadership_lessons_from_Encana_Oil_Gas_USA_Inc

Kölbel, T., Gawlitza, T., & Weinhardt, C. (2022). Shaping Governance in Self-Sovereign Identity Ecosystems: Towards a Cooperative Business Model. *Wirtschaftsinformatik 2022 Proceedings*. https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/18

Kolehmainen, T. (2021). *"Towards a Trustful Digital World: Exploring Self-Sovereign Identity Ec" by Gabriella Laatikainen, Taija Kolehmainen et al.* https://aisel-aisnet-org.kuleuven.e-bronnen.be/pacis2021/19/

Korir, M., Parkin, S., & Dunphy, P. (2022). An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control. *Proceedings of the Eighteenth USENIX Conference on Usable Privacy and Security*, 195–211.

Kuan, K. K. Y., & Chau, P. Y. K. (2001). A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. *Information & Management*, *38*(8), 507–521. https://doi.org/10.1016/S0378-7206(01)00073-8

Kubach, M., Schunck, C. H., Sellung, R., & Roßnagel, H. (2020). *Self-sovereign and Decentralized identity as the future of identity management?*

Kubach, M., & Sellung, R. (2021). *On the Market for Self-Sovereign Identity: Structure and Stakeholders*. Open Identity Summit. https://www.semanticscholar.org/paper/On-the-Market-for-Self-Sovereign-Identity%3A-and-Kubach-Sellung/1c465c5d893c0837c3bd956122af1e2e35b59655

Kubicek, H., & Noack, T. (2010). Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. *Identity in the Information Society*, *3*(1), 235–245. https://doi.org/10.1007/s12394-010-0063-x

Laatikainen, G., Mustak, M., & Hickman, N. (2025). Self-sovereign identity adoption: Antecedents and potential outcomes. *Technology in Society*, *82*, 102859. https://doi.org/10.1016/j.techsoc.2025.102859

Laita, A., & Belaissaoui, M. (2017). Information Technology Governance in Public Sector Organizations. In *Europe and MENA Cooperation Advances in Information and Communication Technologies* (pp. 331–340). Springer, Cham. https://doi.org/10.1007/978-3-319-46568-5_34

Leosk, N., Põder, I., Schmidt, C., Kalvet, T., & Krimmer, R. (2021). Drivers for and Barriers to the Cross-border Implementation of the Once-Only Principle. In *The Once-Only Principle* (pp. 38–60). Springer, Cham. https://doi.org/10.1007/978-3-030-79851-2_3

Liang, H., Wang, J.-J., Xue, Y., & Cui. (2016). *IT outsourcing research from 1992 to 2013: A literature review based on main path analysis—ScienceDirect*. https://www-sciencedirect-com.kuleuven.e-bronnen.be/science/article/pii/S037872061500110X?via%3Dihub

Liesbrock, P., & Sneiders, E. (2024). Assessing Poor Adoption of the eID in Germany. *Information Systems and Technologies*, 292–301. https://doi.org/10.1007/978-3-031-45648-0_29

Lips, A. M. B., Taylor ,John A., & and Organ, J. (2009). Managing Citizen Identity Information in E-Government Service Relationships in the UK: The emergence of a

Surveillance State or a Service State? *Public Management Review*, *11*(6), 833–856. https://doi.org/10.1080/14719030903318988

Lips, S., Bharosa, N., & Draheim, D. (2020). eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. *Electronic Governance and Open Society: Challenges in Eurasia*, 75–89. https://doi.org/10.1007/978-3-030-67238-6_6

Lockwood, M. (2021). Exploring Value Propositions to Drive Self-Sovereign Identity Adoption. *Frontiers in Blockchain*, *4*. https://doi.org/10.3389/fbloc.2021.611945

Lukkien, B., Bharosa, N., & De Reuver, M. (2023). Barriers for developing and launching digital identity wallets. *Proceedings of the 24th Annual International Conference on Digital Government Research*, 289–299. https://doi.org/10.1145/3598469.3598501

Mahula, S., Tan, E., Crompvoets, J., & Timmers, P. (2024). What motivates public sector organisations to use blockchain? *International Journal of Public Sector Management*, *38*(1), 118–138. https://doi.org/10.1108/IJPSM-12-2023-0361

Marconi, V. C., Kaiser, B. N., & Hennink, M. M. (2016). *Code Saturation Versus Meaning Saturation—Monique M. Hennink, Bonnie N. Kaiser, Vincent C. Marconi, 2017*. https://journals-sagepub-com.kuleuven.e-bronnen.be/doi/full/10.1177/1049732316665344

Mariën, I., & Van Audenhove, L. (2010). The Belgian e-ID and its complex path to implementation and innovational change. *Identity in the Information Society*, *3*(1), 27–41. https://doi.org/10.1007/s12394-010-0042-2

Marsman, H., Klenk, M., de Reuver, M., & Bharosa, N. (2024). *How does the EU Digital Identity Wallet change the risk of over-sharing data? A Dutch perspective.*

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, *36*(4), 101385. https://doi.org/10.1016/j.giq.2019.06.002

Michael, K., & Michael, M. (2006). *Historical lessons on ID technology and the consequences of an unchecked trajectory*. https://doi.org/10.1080/08109020601029938']

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Neirotti, P., & Raguseo, E. (2017). On the contingent value of IT-based capabilities for the competitive advantage of SMEs: Mechanisms and empirical evidence. *Information & Management*, *54*(2), 139–153. https://doi.org/10.1016/j.im.2016.05.004

Olutoyin, O., & Flowerday, S. (2016). Successful IT governance in SMES: An application of the Technology-Organisation-Environment theory : original research. *South African Journal of Information Management*, *18*(1), 1–8. https://doi.org/10.4102/sajim.v18i1.696

Panagiotopoulos, P., Klievink, B., & Cordella, A. (2019). Public value creation in digital government. *Government Information Quarterly*, *36*(4), 101421. https://doi.org/10.1016/j.giq.2019.101421

Parker, C., Scott, S., & Geddes, A. (2019). Snowball Sampling. *SAGE Research Methods Foundations*. http://methods.sagepub.com/foundations/snowball-sampling

Parker, G., Van Alstyne, M., & Jiang, X. (2017). Platform Ecosystems: How Developers Invert the Firm. *MIS Quarterly*, *41*(1), 255–266.

Peffers, K., Tuunanen, T., & Rothenberger, M. A. (2007). *A design science research methodology for information systems research*. ResearchGate. https://www.researchgate.net/publication/284503626_A_design_science_research_methodology_for_information_systems_research

Picazo-Vela, S., Luna, D. E., Gil-Garcia, J. R., & Luna-Reyes, L. F. (2022). Creating Public Value Through Inter-Organizational Collaboration and Information Technologies. *International Journal of Electronic Government Research (IJEGR)*, *18*(1), 1–18. https://doi.org/10.4018/IJEGR.288069

Podgorelec, B., Alber, L., & Zefferer, T. (2022). What is a (Digital) Identity Wallet? A Systematic Literature Review. *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 809–818. https://doi.org/10.1109/COMPSAC54236.2022.00131

Pool, R. L. D., Berkel, J. van, & Braak, S. W. van den. (2018). *A conceptual framework for addressing IoT threats: Challenges in meeting challenges*.

Pouloudi, N., & Kalliamvakou, E. (2011). Tracing Diversity in the History of Citizen Identifiers in Europe: A Legacy for Electronic Identity Management? In *Emerging Themes in Information Systems and Organization Studies* (pp. 333–346). Physica-Verlag HD. https://doi.org/10.1007/978-3-7908-2739-2_26

PRISMA STATEMENT. (2020). *PRISMA Statement Diagram*. PRISMA Statement. https://www.prisma-statement.org

Rai, A., Keil, M., Hornyak, R., & Wüllenweber. (2014). *Hybrid Relational-Contractual Governance for Business Process Outsourcing: Journal of Management Information*

Systems: Vol 29, No 2. https://www.tandfonline.com/doi/abs/10.2753/MIS0742-1222290208

Ramona, P. (2021). *Revision of the eIDAS Regulation: Findings on its implementation and application*.

Ranganathan, C., & Balaji, S. (2018). *"Critical Capabilities for Offshore Outsourcing of Information Systems" by C. Ranganathan and S. Balaji*. https://aisel-aisnet-org.kuleuven.e-bronnen.be/misqe/vol6/iss3/4/

Raschke, R. L., & Sen, S. (2013). *A value-based approach to the ex-ante evaluation of IT enabled business process improvement projects—ScienceDirect*. https://www-sciencedirect-com.kuleuven.e-bronnen.be/science/article/pii/S0378720613000797?via%3Dihub

Reichstädter, P. (2003). E-Signatures for Delivery in e-Government. *Electronic Government*, 260–265. https://doi.org/10.1007/10929179_47

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Sedlmeir, J., & Weigl, L. (2022). *Transition Pathways towards Design Principles of Self-Sovereign Identity*.

Sharma, S., & Mishra, N. K. (2011). New Innovations in Cryptography and Its Applications. *High Performance Architecture and Grid Computing*, 527–538. https://doi.org/10.1007/978-3-642-22577-2_71

Shehu, A., Pinto, A., & Correia, M. E. (2019). On the Interoperability of European National Identity Cards. *Ambient Intelligence – Software and Applications –, 9th International Symposium on Ambient Intelligence*, 338–348. https://doi.org/10.1007/978-3-030-01746-0_40

Shoshana, Z. (2015). *Big other: Surveillance Capitalism and the Prospects of an Information Civilization*. https://doi.org/10.1057/jit.2015.5

Smith, H. A., & McKeen, J. D. (2018). *"Creating a Process-Centric Organization at FCC: SOA from the Top Down" by Heather A. Smith and James D. McKeen*. https://aisel-aisnet-org.kuleuven.e-bronnen.be/misqe/vol7/iss2/4/

Sroor, M., Hickman, N., Kolehmainen, T., Laatikainen, G., & Abrahamsson, P. (2022). How modeling helps in developing self-sovereign identity governance framework: An

experience report. *Procedia Computer Science*, *204*, 267–277. https://doi.org/10.1016/j.procs.2022.08.032

Svahn, F., Mathiassen, L., & Lindgren, R. (2017). Embracing digital innovation in incumbent firms: How volvo cars managed competing concerns. *MIS Q.*, *41*(1), 239–253. https://doi.org/10.25300/MISQ/2017/41.1.12

Twizeyimana, J. D., & Andersson, A. (2019). The public value of E-Government – A literature review. *Government Information Quarterly*, *36*(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2014a). Designing Privacy-by-Design. *Privacy Technologies and Policy*, 55–72. https://doi.org/10.1007/978-3-642-54069-1_4

van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2014b). Designing Privacy-by-Design. *Privacy Technologies and Policy*, 55–72. https://doi.org/10.1007/978-3-642-54069-1_4

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

Weigl, L., Amard, A., Codagnone, C., & Fridgen, G. (2022). The EU's Digital Identity Policy: Tracing Policy Punctuations. *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*, 74–81. https://doi.org/10.1145/3560107.3560121

Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. *Government Information Quarterly*, *40*(4), 101873. https://doi.org/10.1016/j.giq.2023.101873

Weigl, L., & Reysner, M. (2024). The Governance of the European Digital Identity Framework Through the Lens of Institutional Mimesis. *Regulation & Governance*, *n/a*(n/a). https://doi.org/10.1111/rego.70032

Weston, C., Gandell, T., Beauchamp, J., McAlpine, L., Wiseman, C., & Beauchamp, C. (2001). Analyzing Interview Data: The Development and Evolution of a Coding System. *Qualitative Sociology*, *24*(3), 381–400. https://doi.org/10.1023/A:1010690908200

Whitley, E. A., & Schoemaker, E. (2022). On the sociopolitical configurations of digital identity principles. *Data & Policy*, *4*, e38. https://doi.org/10.1017/dap.2022.30

Wilkin, C. L., & Chenhall, R. H. (2020). Information Technology Governance: Reflections on the Past and Future Directions. *Journal of Information Systems*, *34*(2), 257–292. https://doi.org/10.2308/isys-52632

Xue, L., Ray, G., & Gu, B. (2011). Environmental Uncertainty and IT Infrastructure Governance: A Curvilinear Relationship. *Information Systems Research*, *22*(2), 389–399. https://doi.org/10.1287/isre.1090.0269

Appendix

A Literature review concept map

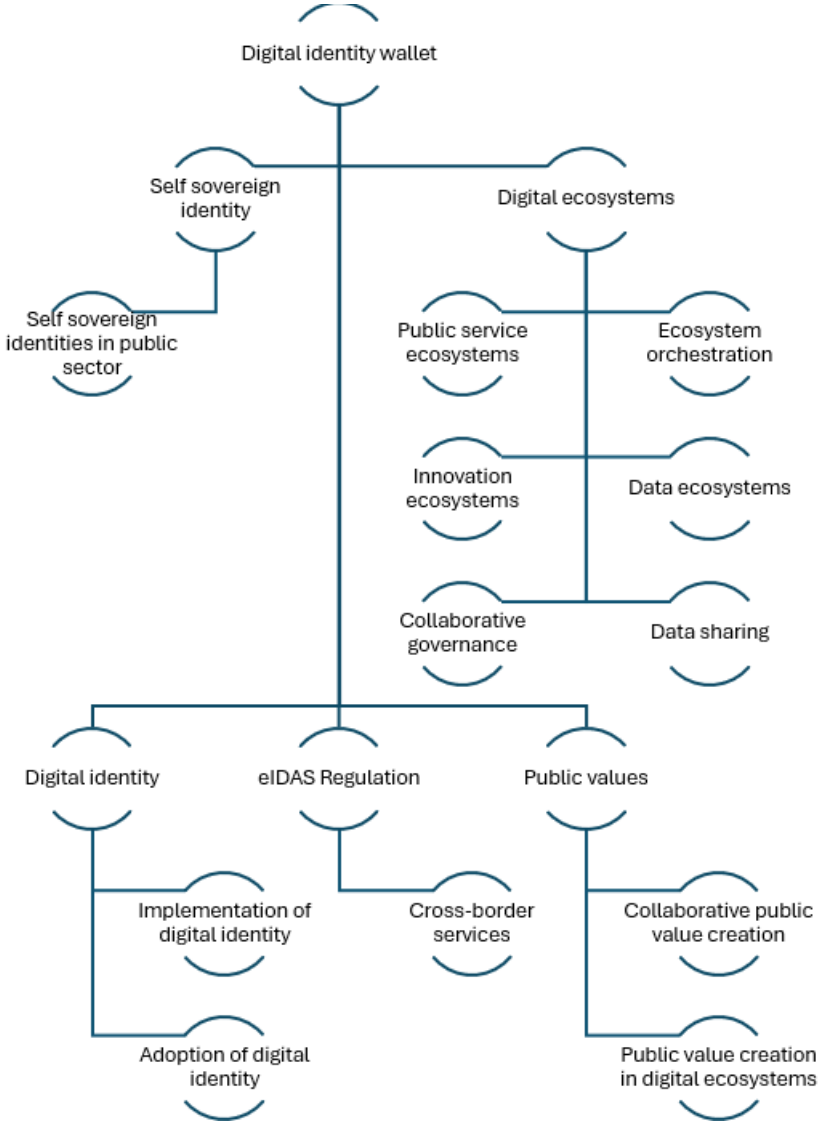

Figure 12 Literature review concept map Author's elaboration

B Literature review concept matrix

Articles	Public value	SSIs	Data ecosystem	Innovation	Digital transformation	Orchestration	Super app	Socio technical system	VCs	PKI	Privacy protection	Data protection	Business models	Good governance	Public private ecosystem	Flexibility	Implementation	Data sovereignty
Weigl & Reysner, 2025		X																
Degen & Teubner, 2024	X	X	X		X	X	X						X					

Weigl et. al., 2023	X				X		X		X	X	X						X								
Giannopoulou & Wang 2021	X	X							X		X														
Kubach et. al., 2020	X	X							X	X			X		X		X								
Köbel et. al., 2022	X	X							X		X		X		X		X								
Sedlmeir & Weigl, 2022	X		X						X	X			X		X								X		X
Lukkien et. al., 2023	X																			X					
Giannopoulou, 2023	X	X							X		X		X		X										

Table 5 Literature review concept matrix Author's elaboration

C Literature review PRISMA diagram

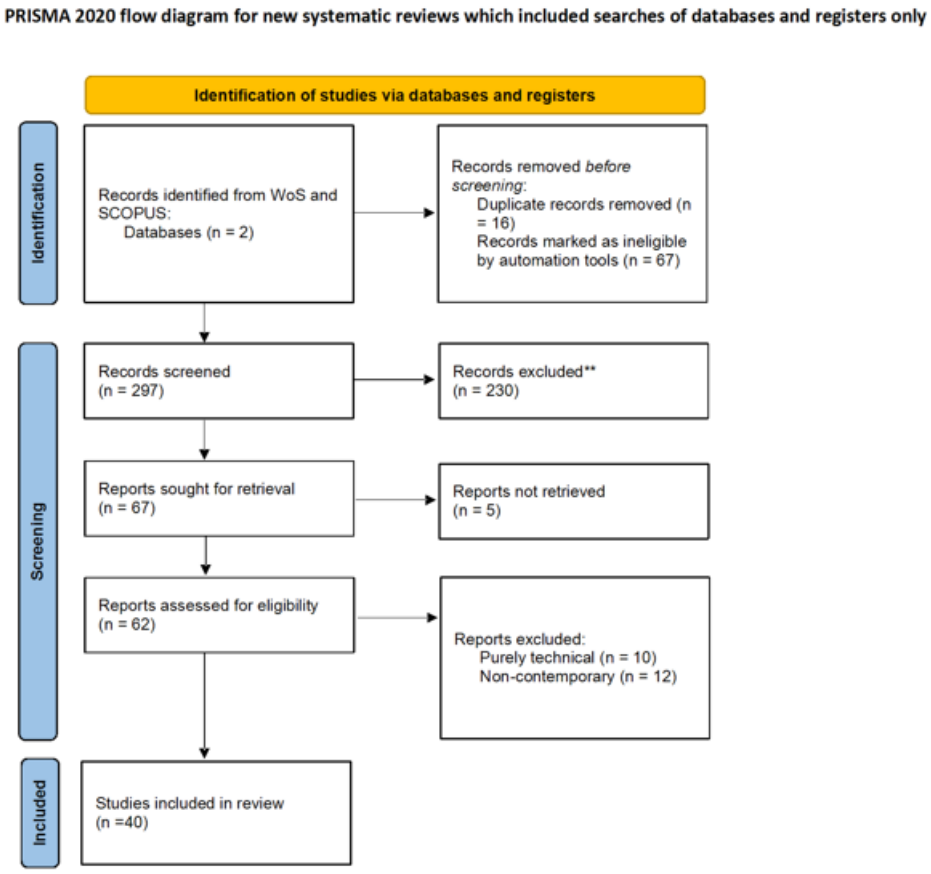

Figure 13 Literature review PRISMA diagram From (PRISMA STATEMENT, 2020)

D Conceptual dimensions of EUDIF ecosystem actors

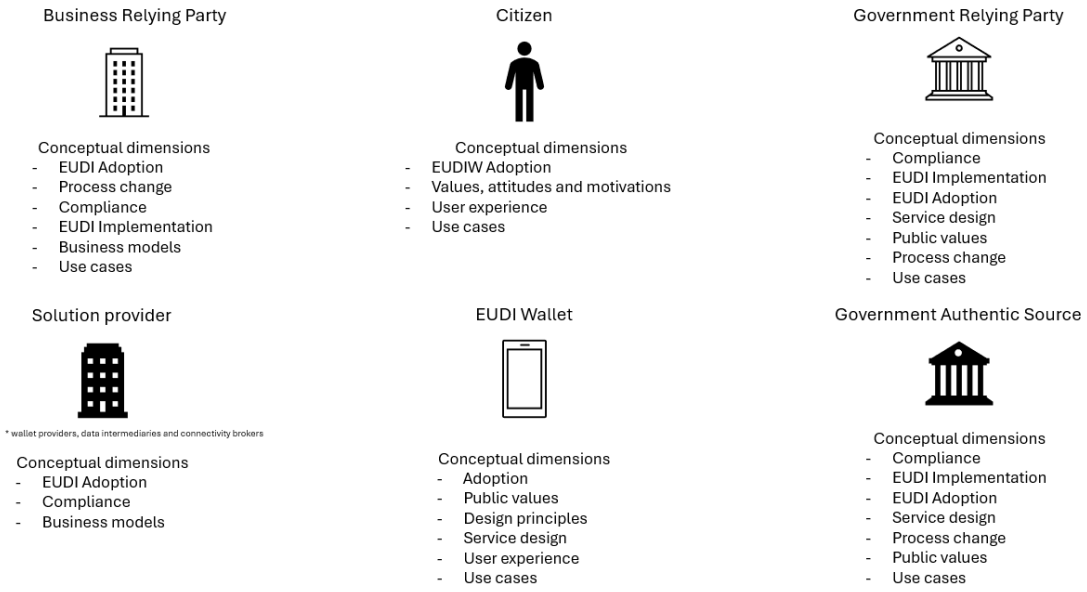

Figure 14 EUDIF ecosystem actors Adapted from (Degen & Teubner, 2024)

E Table of interview participants

Interview ID	Role	Organizational ecosystem role	Phase	Duration (in minutes)
1	eIDAS Expert	Solution provider	P1	34
2	CEO	Solution provider	P1	29
3	Trust services consultant	Consultancy	P1	81
4	Public sector trust services consultant	Consultancy	P1	29
5	Business developer	Solution provider	P1	49
6	CEO	Solution provider	P1	30
7	Senior advisor	Public sector	P1	31
8	Consultant	Consultancy	P1	51
9	Program manager	Public sector	P1	29
10	Program manager	Public sector	P1	38
11	Identity architect	Public sector	P1	29

12	Senior policymaker	Public sector	P1	79
13	Business manager	Solution provider	P1	20
14	Identity architect	Public sector	P1	70
15	Advisor	Public sector	P1	49
16	Senior advisor	Public sector	P1	52
17	Strategic advisor	Public sector	P1	34
18	UX designer	Public sector	P2	41
19	Enterprise architect	Consultancy	P2	30
20	Program manager	Public sector	P2	39
21	Program manager	Public sector	P2	38
22	CTO	Solution provider	P2	23
23	Strategic advisor	Public sector	P2	53
24	Researcher	Infrastructure provider	P2	29
25	Director	Solution provider	P2	21
26	Founder	NGO	P2	24
27	Innovation director	Solution provider	P2	29
28	Researcher	University	P2	26

Table 6 Interview partners Author's elaboration

F Tabled results of first evaluation phase semi-structured interviews

Table 7 Results of first evaluation phase semi-structured interviews Author's elaboration

Ecosystem role	Levels of analysis	Observation	Theme(s)
	Ecosystem	Barrier(s)	Lack of [certification schemes, investment, engagement programs, awareness] chicken-egg problem, high compliance requirements, high initial investment, bare minimum approach to EUDIF
	Ecosystem	Driver(s)	Economic benefits, reuse of authentic data

Service provider	Organization	Barrier(s)	Lack of use cases, fast pace of regulatory developments, compliance burdens, additional liability
	Organization	Driver(s)	Process efficiency, compliance
	Individual	Barrier(s)	Complexity, existing solutions, lack of [use cases, digital identity use frequency] incumbent methods of digital identification
	Individual	Driver(s)	N/A
	Ecosystem	Barrier(s)	Lack of certification schemes fast paced regulatory developments, low readiness, incompatible business models
	Ecosystem	Driver(s)	Wallet data sharing capabilities, economic benefits, lowering compliance requirements, private sector ecosystem participation
Public sector organization	Organization	Barrier(s)	Bare-minimum approach to adoption, lack of [use cases, vision, management support]
	Organization	Driver(s)	Mandatory acceptance, process efficiency, cost savings, domain organizations, management support, public value creation, mandate fulfilment, increased security
	Individual	Barrier(s)	Low digital literacy, complexity, existing solutions, lack of [use cases, perceived need]
	Individual	Driver(s)	Relevant services, cross-border use cases

G Axial code frequency distribution between EUDIF ecosystem actors

Axial codes signify directionality of statements. For example, a challenge identified as exhibited in private sector relying parties by a public sector representative has been coded as: public sector – private sector relying parties [open code of identified challenge]. Below is a chart of axial code distributions with directionality towards EUDIF ecosystem participator roles elaborated entirely from our codebook enclosed in the appendix.

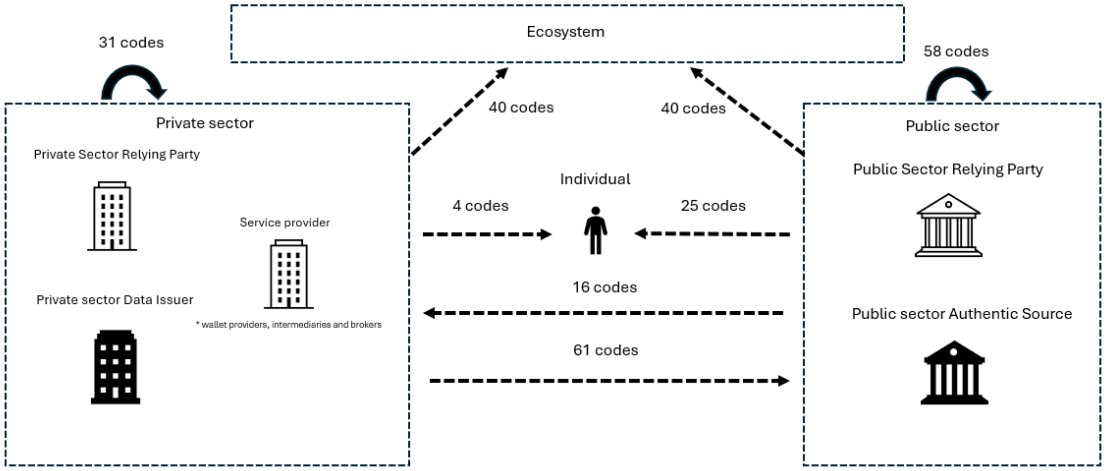

Figure 15 Axial code frequency distribution Author's elaboration

H Codebook

Name	Description	Files	References
access security and identity assurance as an adoption driver in public sector		1	1
actions to be taken for wallet adoption readiness at local government level		1	1
additional oversight required to govern non registered relying parties		1	1
effects of wallets on government workflows		1	1
antecedents of organizational EUDI adoption		1	1
antecedents to enabling data sharing ecosystem with EUDIW		1	1
approach to digital transformation to support business cases		1	1
approach to IT value creation with frameworks in local government		1	1
approach to wallet adoption in private sector		1	1

Name	Description	Files	References
architectural changes to support service connectivity problems		1	1
attestation as the driver of the EUDI ecosystem		1	1
attribute sharing potentially a breaking change for business processes		1	1
authentic data as a driver for KYC processes		1	1
authentic data availability as an adoption driver		1	1
authentic source competencies in Belgium		1	1
availability of attribute validation systems as a matter of trust		1	1
awareness around privacy issues		1	1
awareness levels of critical industries		1	1
awareness levels of Dutch public sector towards eudif		1	1
awareness levels of federal government		1	1
awareness levels of private companies on eudif		1	1
awareness of Dutch public sector		1	1
awareness of eudif offerings and motivation to adopt federal level building blocks		1	1
awareness of local governments on self-sovereign identity principles		1	1
balancing interests in local level eudiw adoption		1	1
benefits of having access to authentic data		1	1
benefits of wallet adoption for g2c and g2b use cases		1	1
board support importance for eudif adoption		1	1
business model enablement in eudif ecosystem as public value		1	1

Name	Description	Files	References
business models of data providers are not structured to provide data in credential format		1	1
capabilities of the wallet to provide solutions to stakeholder problems		1	1
capability modelling on better program alignment in the Netherlands		1	1
challenge of technical implementation of regulatory requirements		1	1
challenges and features of data exchange between data consumer and provider organizations on the Netherlands		1	1
challenges and gaps in public procurement and requirements management in local governments towards eudiw		1	1
challenges for business adoption of authentic data		1	1
challenges of co-opting each other's services in multi governance level in Belgium		1	1
challenges of cross border use case adoption of eudif for local governments		1	1
challenges of enacting attestation validation services in Belgium		1	1
challenges of ensuring interoperability as organizations follow different timelines		1	1
challenges of enterprise architecture practice in local government		1	1
challenges of eudiw migration in the public sector		1	1
challenges of fast changing requirements environment on public procurement		1	1

Name	Description	Files	References
challenges of multi layered government structure in eudif implementation		1	1
challenges of multi-level governance with eudif rollout in Belgium		1	1
challenges of open code approach		1	1
challenges of overfocusing on regulation in digital transformation		1	1
challenges of selective disclosure in audits		1	1
challenges with accessing authentic data		1	1
challenges with authentic source connectivity of Dutch municipalities		1	1
challenges with authentic source authentication		0	0
challenges with authentic source authentication		1	1
challenges with enacting interoperability for authentic source connectivity for local governments		1	1
change in analogue modes of process design		1	1
chicken and egg problem of identity attributes		1	1
CIRs introducing breaking changes to business models		1	1
CIRs introducing breaking changes to operational trust services		1	1
collaboration aspects of eudif rollout in Belgium		1	1
common governance challenges in the Belgian context		1	1
communication on wallet rollout initiatives		1	1
companies focusing on process level changes instead of ecosystem adoption		1	1

Name	Description	Files	References
competencies to ecosystem participation		1	1
competition elements exist to make relying parties transform		1	1
competition elements do not exist for attribute registries		1	1
complexity of having decentralized registries		1	1
concerns for stringent regulation blocking use cases		1	1
conditions and constraints of relying party adoption to the wallet ecosystem		1	1
conditions for attribute providers and PPP models for attribute providers and local governments		1	1
context of public value in eudiws		1	1
creation of incentives for eudiw digital transformation		1	1
data availability challenges limiting eudiw uptake		1	1
data use for proactive public service delivery in local governments		1	1
decentralization of public procurement process knowledge		1	1
development of eID means capabilities with the EUDI		1	1
differences in analogue vs digital process design		1	1
distribution of use cases across B2B and B2G		1	1
division of responsibilities towards eudif in Belgium		1	1
drive to merely accept EUDIW as identification		1	1
Dutch central government ability to deliver mobile driver licenses to wallets		1	1
Dutch perception on ecosystem readiness		1	1

Name	Description	Files	References
Dutch perspective on relying parties information handling		1	1
dynamics of ecosystem building		1	1
EAA embedded policies enabling relying party trust on EAA verification		1	1
EAAs addressing trust problems of common artifacts		1	1
EAAs allowing new solutions		1	1
EAAs allowing private sector relying party use cases		1	1
EAAs are important for data sharing solutions		1	1
EAAs as government use case drivers		1	1
EAAs enabling a trust framework for identity attributes		1	1
EAAs enabling cross border non-governmental data sharing		1	1
EAAs enabling economic value and user friendliness		1	1
EAAs enabling increased data confidentiality		1	1
EAAs enabling seamless business processes in public sector		1	1
EAAs introducing legal recognition and automation capability		1	1
ecosystem information asymmetries		1	1
ecosystem needs beyond orchestration		1	1
ecosystem uncertainties around trust roles and schemes		1	1
EEAs enabling private sector relying party use cases with selective disclosure		1	1

Name	Description	Files	References
effect of frequent use on digital identity adoption		1	1
effects of achieving high level of assurance on ecosystem participation		1	1
effects of multiple wallets on ecosystem orchestration complexity		1	1
eidas trust framework to harmonize trust in government processes		1	1
EU regulations controlling over asking		1	1
EUDI adoption strategies in public sector		1	1
EUDI adoption tied to networks effects		1	1
EUDI introducing new technical capabilities		1	1
eudif adoption being an organizational change		1	1
eudif as a public value creation mechanism		1	1
eudif getting rolled out in active engagement to mitigate national law alignment issues		1	1
eudif governance aspects of Belgian rollout		1	1
eudif requirements introducing challenges for implementation		1	1
eudif rollout multi-level governance in the Netherlands		1	1
eudiw adoption as an opportunity for process refactoring		1	1
eudiw capabilities introducing process efficiency		1	1
eudiw wallet as a central trust component in the eudif ecosystem		1	1
eudiw wallet as empowerment for individuals		1	1

Name	Description	Files	References
eudiw wallet capabilities to limit process biases		1	1
Exclusive ecosystems focus on EUDIW		1	1
fast pace of regulatory developments being pushed to the ecosystem		1	1
federal government interactions with other levels regarding eudiw use in Belgium		1	1
federated service connectivity in the Netherlands and its relation to OOTS and wallets		1	1
focus on citizen use cases in Belgium		1	1
foreseen capabilities for the Belgian eudiw		1	1
fundamental division of responsibilities in the Netherlands		1	1
gaps in current ITG practice in local government		1	1
gaps in ecosystem role definitions		1	1
gaps in organizational decision-making capability around eudiw adoption		1	1
gaps in structural maturity to govern eudiw		1	1
governance aspects of authentic sources in Belgian eudif rollout		1	1
governance aspects of digital identities in Belgium		1	1
government authentic data enabling KYC business cases		1	1
government registry data as a business case enabler		1	1
government's role in building the Dutch eudiw ecosystem		1	1
hands on approach to digital transformation		1	1

Name	Description	Files	References
having a regulatory first focus to eidas centered digital transformation		1	1
hesitant behaviour of critical sectors to engage with the wallet		1	1
immature enterprise architecture practice in Dutch authorities		1	1
immature nature of regulatory developments		1	1
impact of enterprise architecture practice towards digital transformation goals		1	1
impact of legacy systems on change management		1	1
Implementation challenges due to regulation immaturity		1	1
implementation of eudif in the Netherlands delineated between authorities		1	1
importance of creating trust with citizens during eudiw implementation		1	1
importance of delivering consistent user experience with eudiw		1	1
importance of having stakeholder support for eudiw adoption		1	1
importance of multi-level collaboration to deliver value in Belgium eudif rollout		1	1
importance of natural to legal person mandate attestations in Belgian context		1	1
importance of reaching out to domain organizations		1	1
importance of the government stakeholder role in Belgian context		1	1
indication of local government working with PPPs for the wallet		1	1

Name	Description	Files	References
indication of local governments practicing data issuance		1	1
individual heuristics of public service delivery clashing with eudiw		1	1
individual level data control concerns		1	1
individual level wallet adoption against incumbent ID platforms		1	1
individual trust in the government challenging wallet adoption		1	1
individual wallet adoption challenges		1	1
intermediary data sharing use cases enabled by consent mechanism		1	1
inventive strategies for data providers		1	1
involvement of local levels is crucial in Belgian eudif rollout		1	1
joint perspective preference on eudif		1	1
KYC as a cross sectoral business case		1	1
lack of a central vision for the eudif project in the Netherlands		1	1
lack of common standards for authentic source access		1	1
lack of concrete definitions of artifacts to enable more business cases		1	1
lack of eudif awareness from the public sector		1	1
lack of incentives for public sector managers around eudiw digital transformation		1	1
lack of use cases on the delivery of business cases		1	1
lacking funding structures		1	1
learnings from other ecosystems		1	1

Name	Description	Files	References
legal requirements being drivers for eidas digital transformation		1	1
linear progression of digital transformation activities		1	1
local government readiness to data sharing		1	1
maturity levels of eudif capabilities		1	1
means for users to authenticate to public services in Belgium		1	1
mechanisms to engage wallet providers early on		1	1
models to build trust relationships with individuals in local government context		1	1
modes of creating trust with data management in local government		1	1
motivation to inherit trust from public data issuers with collaborations		1	1
motivation to utilize the wallet in the Dutch public sector		1	1
multi-party transactions relevancy to governments		1	1
national legislation not adjusted for eudif		1	1
nature of digital identification competencies in Belgium		1	1
nature of regional and local interactions with eudif in Belgium		1	1
necessity for transformation in public sector to issue attributes		1	1
necessity of stakeholder communication of process changes due to wallet adoption in local government		1	1
need for transparency on data use cases		1	1
public sector - ecosystem		1	1

Name	Description	Files	References
enablement of business models in eudif ecosystem as public value			
no guidelines for private sector relying parties for wallet adoption		1	1
non-existent certification schemes for new trust products		1	1
nudging users towards eudiw use with disclaimers		1	1
obligation as a driver for eudif adoption		1	1
opportunities of eudif adoption for Dutch public sector		1	1
participation of private parties in the EUDI ecosystem		1	1
past engagements and awareness levels of public sector around eudif		1	1
perceived benefits of having a holistic view of the eudif ecosystem		1	1
perception of a need for a proactive response against oversharing in local government		1	1
perception of a need for stakeholder communication around technical details for organization wallet adoption at local government		1	1
perception of antecedents for ecosystem uptake		1	1
perception of business drivers behind company wallets for local government use cases		1	1
perception of business value with eudiw		1	1
perception of demoing eudiw with users for better adoption		1	1
perception of dependency on PPPs to deliver wallet functionality		0	0

Name	Description	Files	References
perception of dependency on PPPs to deliver wallet functionality		1	1
perception of digital identity use primarily motivated by use frequency with private sector use cases		1	1
perception of eudif rollout in Belgium		1	1
perception of governments role in eudif ecosystem		1	1
perception of lacklustre use cases for wallet while alternative means exist		1	1
perception of laws hindering data flows		1	1
perception of limited scope for eudiw rollout in the Netherlands		1	1
perception of public sector motivation on compliance		1	1
perception of risk-based access control for local governments		1	1
perception of technical adoption requirements for eudiw at local government level		1	1
perception of use case value with eudiw		1	1
perception of use of multiple attributes potentially a breaking change for business processes		1	1
perception of value for company wallet adoption for local government use cases		1	1
perception on digital transformation strategies		1	1
perception on role of the government in eudif ecosystem		1	1
perception on wallet as a process value creation enabler		1	1

Name	Description	Files	References
perceptions of how individual attitudes on eudiw is formed		1	1
perceptions on a eudif transformation governance framework		1	1
perspective on user centric operation of the eudiw		1	1
PID as the primary driver for the attestation ecosystem		1	1
policy organizations supporting rollout with building blocks in Belgium		1	1
political effects in eudif rollout in Belgium		1	1
possible configuration models for wallet ecosystem		1	1
PPPs focus on delivering software		1	1
PPPs in digital identities creating facilitating conditions for adoption		1	1
practicalities of dealing with national law		1	1
previous public sector management experience helping in eudif adoption in the government		1	1
private parties' participation in national wallet as an adoption driver		1	1
private sector eudif uptake depends on business models and opportunities		1	1
private sector role in eudif rollout in the Netherlands		1	1
process enactment to practice selective disclosure in local government		1	1
process enactment towards wallet use cases for g2b		1	1
process of digital transformation		1	1
process redesign relevancy to wallet adoption		1	1

Name	Description	Files	References
process requirements defined by law		1	1
public sector - public sector challenges with authentic source authentication		1	1
public sector - authentic source providers strategies to incentivise data providers		1	1
public sector - data providers competition element does not exist for attribute providers in the Netherlands		1	1
public sector - ecosystem business models of authentic data providers not adapted to provide data in credential format		1	1
public sector - ecosystem capabilities of the wallet to provide solutions for stakeholders		1	1
public sector - ecosystem challenges and models for data exchange between data provider and data consumer organizations in the Netherlands		1	1
public sector - ecosystem challenges of cross border use cases of eudiw in local governments		1	1
public sector - ecosystem challenges of multi-level governance structures on eudif implementation in the Netherlands		1	1
public sector - ecosystem constraints and challenges of relying party access to the EUDI ecosystem		1	1
public sector - ecosystem context of public value in eudiws		1	1
public sector - ecosystem Dutch perception on ecosystem readiness		1	1
public sector - ecosystem ecosystem information asymmetries		1	1

Name	Description	Files	References
public sector - ecosystem ecosystem needs beyond orchestration		1	1
public sector - ecosystem ecosystem uncertainties around roles and schemes		1	1
public sector - ecosystem effects of achieving high level of assurance on ecosystem participation		1	1
public sector - ecosystem effects of multiple wallet configurations on ecosystem orchestration complexity		1	1
public sector - ecosystem federated service connectivity and its relation to OOTS and wallets		1	1
public sector - ecosystem focus on citizen use cases in Belgium		1	1
public sector - ecosystem gaps in ecosystem role definitions		1	1
public sector - ecosystem gaps in organizational decision-making ability to assess eudiw adoption fit		1	1
public sector - ecosystem governments role in building the Dutch eudiw ecosystem		1	1
public sector - ecosystem immature nature of regulatory developments		1	1
public sector - ecosystem importance of reaching out to domain organizations		1	1
public sector - ecosystem indication for local governments working with PPPs for wallet		1	1
public sector - ecosystem indication that local governments practice data issuance		1	1
public sector - ecosystem joint perspectives preferred for eudif		1	1

Name	Description	Files	References
public sector - ecosystem lack of a central vision for the eudif ecosystem in the Netherlands		1	1
public sector - ecosystem learnings from other ecosystems		1	1
public sector - ecosystem need for transparency on data use cases		1	1
public sector - ecosystem perception of antecedents for ecosystem uptake		1	1
public sector - ecosystem perception of laws hindering data flows		1	1
public sector - ecosystem political effects in eudif rollout in Belgium		1	1
public sector - ecosystem possible configurations on eudiw in the ecosystem		1	1
public sector - ecosystem private sector role in eudif rollout in the Netherlands		1	1
public sector - ecosystem public sector focus on delivering IT and compliance instead of ecosystem orchestration		1	1
public sector - ecosystem readiness to issue PIDs in Belgium		1	1
public sector - ecosystem regulation and government structure as a limitation on business models		1	1
public sector - ecosystem regulatory immaturity as an eudif adoption readiness challenge		1	1
public sector - ecosystem relevancy of credentials affecting adoption		1	1
public sector - ecosystem role of government in eudif ecosystem		1	1
public sector - ecosystem strategies for creating support systems		1	1

Name	Description	Files	References
public sector - ecosystem strategies for orchestrators		1	1
public sector - ecosystem wallet operation challenged by business models for authentic source providers		1	1
public sector - individual data use for proactive public service delivery in local governments		1	1
public sector - individual eudiw capabilities to limit process biases		1	1
public sector - individual individual heuristics of public service delivery clashing with eudiw		1	1
public sector - individual modes of creating trust with data management		1	1
public sector - individual perception of demoing eudiw for better individual adoption		1	1
public sector - individual utilizing citizen trust built at local levels for legitimacy building		1	1
public sector - individuals awareness around privacy issues		1	1
public sector - individuals challenges with individual trust in the government with eudiw adoption		1	1
public sector - individuals eudiw as individual empowerment		1	1
public sector - individuals importance of creating trust with individuals during eudiw implementation		1	1
public sector - individuals importance of delivering consistent user experience with eudiw		1	1
public sector - individuals individual level data control problems		1	1

Name	Description	Files	References
public sector - individuals methods for authentication to public services in belgium		1	1
public sector - individuals models to build trust relationships with individual users in local government		1	1
public sector - individuals necessity of stakeholder communication for process changes due to wallet adoption in local governments		1	1
public sector - individuals nudging users towards eudiw with disclaimers		1	1
public sector - individuals perception of a need for stakeholder communication around technical details for organization wallet adoption at local government		1	1
public sector - individuals perception of risk-based access control for local governments		1	1
public sector - individuals perception of wallet adoption for individuals going against incumbent ID platforms		1	1
public sector - individuals perception on importance of mechanisms against oversharing by individuals		1	1
public sector - individuals perspective on user centric operation of eudiw		1	1
public sector - individuals process enactment to practice selective disclosure in local governments		1	1
public sector - individuals stakeholder communication of digital identification means change in local government		1	1

Name	Description	Files	References
public sector - individuals value propositions of wallet choice		1	1
public sector - individuals wallet capabilities changing usual service delivery processes		1	1
public sector - private sector authentic data as a KYC use case driver		1	1
public sector - private sector perception of dependency on private sector PPPs for wallet functionality		1	1
public sector - private sector perception of use case value for company wallet adoption for local government use cases		1	1
public sector - private sector private sector participation in national wallet as a use case driver		1	1
public sector - private sector process enactment to enable business user use cases in local governments		1	1
public sector - private sector relying parties competition exist to make relying parties transform		1	1
public sector - private sector relying parties no guidelines available for private sector relying parties for wallet adoption		1	1
public sector - private sector relying parties' perception of business drivers for company wallets for local government use cases		1	1
public sector - private sector relying parties reuse of authentic data as a business driver		1	1
public sector - private sector status of PPPs around the use of eudiw in Belgium		1	1

Name	Description	Files	References
public sector - public sector access security and identity assurance as an adoption driver in local government		1	1
public sector - public sector actions to be taken for wallet adoption at local government level		1	1
public sector - public sector approach to IT value creation with frameworks in local government		1	1
public sector - public sector architectural changes to support service connectivity		1	1
public sector - public sector authentic source competencies in Belgium		1	1
public sector - public sector awareness of the Dutch public sector around eudiw		1	1
public sector - public sector awareness levels of public sector for eudif		1	1
public sector - public sector awareness of eudif offerings and motivation to adopt federal building blocks		1	1
public sector - public sector balancing interests in local eudiw adoption		1	1
public sector - public sector board support for eudif adoption		1	1
public sector - public sector challenges and gaps in procurement and requirements management towards eudiw		1	1
public sector - public sector challenges of ensuring interoperability as organizations follow different timelines		1	1
public sector - public sector challenges of enterprise architecture practice in local government		1	1

Name	Description	Files	References
public sector - public sector challenges of eudiw migration in the public sector		1	1
public sector - public sector challenges with authentic source connectivity of municipalities		1	1
public sector - public sector communication of rollout initiatives		1	1
public sector - public sector complexity of having decentralized registries		1	1
public sector - public sector creating incentives for eudiw digital transformation		1	1
public sector - public sector Dutch central government ability to issue mobile driver licenses to the wallet		1	1
public sector - public sector EAAs as use case drivers for public sector		1	1
public sector - public sector EU regulations controlling over asking		1	1
public sector - public sector eudif adoption being an organizational change		1	1
public sector - public sector eudif ecosystem roles in Belgian public sector		1	1
public sector - public sector eudif rollout multi-level governance in the Netherlands		1	1
public sector - public sector eudiw as an opportunity for process refactoring		1	1
public sector - public sector eudiw capabilities introducing process efficiency		1	1
public sector - public sector federal government interactions with other levels regarding eudiw use in Belgium		1	1

Name	Description	Files	References
public sector - public sector foreseen capabilities of Belgian eudiw		1	1
public sector - public sector fundamental division of responsibilities in the Netherlands		1	1
public sector - public sector gaps in eudiw governance ability		1	1
public sector - public sector gaps in ITG practice in local government		1	1
public sector - public sector impact of enterprise architecture practice towards digital transformation goals		1	1
public sector - public sector importance of delivering consistent user experiences with eudiw		1	1
public sector - public sector internal process improvement as a wallet adoption mechanism in local government		1	1
public sector - public sector lack of incentives for public sector managers around eudiw digital transformation		1	1
public sector - public sector local government awareness on self-sovereign identity principles		1	1
public sector - public sector local government readiness to data sharing		1	1
public sector - public sector maturity levels of eudif capabilities		1	1
public sector - public sector motivation to utilize the wallet in the Dutch public sector		1	1
public sector - public sector nature of digital identification competencies in Belgium		1	1

Name	Description	Files	References
public sector - public sector nature of eudif interactions in regional and local levels of government in Belgium		1	1
public sector - public sector obligation as an adoption driver		1	1
public sector - public sector opportunities of eudiw adoption for Dutch public sector		1	1
public sector - public sector perception of how individual attitudes for eudiw is developed in the Dutch public sector		1	1
public sector - public sector perception of implementation gap where responsibility delineation for implementation exists		1	1
public sector - public sector perception of limited scope for eudiw rollout in the Netherlands		1	1
public sector - public sector perception of technical requirements to wallet adoption at local government level		1	1
public sector - public sector perception on wallet as a process value creation enabler		1	1
public sector - public sector perceptions on a governance framework for eudif		1	1
public sector - public sector public sector IT focus on delivering software instead of ecosystem value		1	1
public sector - public sector relying parties design principles of the wallet as a trust driver		1	1
public sector - public sector slow eudif uptake in Dutch public sector		1	1

Name	Description	Files	References
public sector - public sector small jurisdictions needing support for adoption		1	1
public sector - public sector strategies to initiate adoption mechanisms		1	1
public sector - public sector technical changes to wallet adoption at local government level		1	1
public sector - public sector use of multiple attributes potentially a breaking change for business processes		1	1
public sector - public sector wallet capabilities enhancing data quality in processes		1	1
public sector - public sector wallet enabling value for public sector relying parties		1	1
public sector - relying parties benefits of having access to authentic data		1	1
public sector - relying parties importance of having stakeholder support for eudiw adoption		1	1
public sector - relying parties perspective on relying parties information handling		1	1
public sector - relying parties SD and ZKPs not barriers		1	1
public sector - service providers conditions for attribute providers and PPP models for attribute providers and local government		1	1
public sector capacity to transformation		1	1
public sector digital identities adoption strategies		1	1
public sector eudif ecosystem roles in Belgium		1	1

Name	Description	Files	References
public sector focus on IT delivery and compliance instead of ecosystem orchestration		1	1
public sector on procurement governance		1	1
qtsp liability in electronic transactions		1	1
readiness of private sector organizations to adopt service offering		1	1
readiness to issue PIDs in Belgium		1	1
reasons for complex nature of DPIs in Belgium		1	1
regulation and government structure as a limitation on business models		1	1
regulation immaturity as a challenge for eudif adoption readiness		1	1
regulator - ecosystem chicken and egg problem of identity attributes		1	1
regulator - ecosystem eudif as a public value creation mechanism		1	1
regulator - ecosystem eudiw as a central trust component in the eudif ecosystem		1	1
regulator - ecosystem transparency aspects over issuers		1	1
regulator - private sector eudiw uptake depending on business and use cases		1	1
regulator - public sector analogue vs digital process design		1	1
regulator - public sector capacity to transformation		1	1
regulator - public sector eidas framework to harmonize trust in public sector processes		1	1
regulator - public sector necessity of transformation to issue attributes		1	1

Name	Description	Files	References
regulator - public sector technology adoption modes of public sector		1	1
regulatory requirements challenging small players		1	1
relevancy of credentials affecting adoption		1	1
reuse of authentic data as a business case driver		1	1
reuse of building blocks in the Belgian public sector		1	1
role of government in eudif ecosystem		1	1
role of public sector governance on setting out ecosystems		1	1
role of the government for eudif ecosystem		1	1
SD and ZKPs not barriers for processes		1	1
selective disclosure enabling increased privacy for individuals		1	1
service and technical requirements to adopt a vendor solution		1	1
service provide - service provider EAAs introducing legal recognition and automation capability		1	1
service provider - ecosystem additional oversight required for non-registered relying party use cases		1	1
service provider - ecosystem effects of use frequency on digital identity adoption		1	1
service provider - ecosystem antecedents to enabling data sharing ecosystems with EUDIW		1	1
service provider - ecosystem attributes as the value drivers of the EUDI ecosystem		1	1
service provider - ecosystem authentic data		1	1

Name	Description	Files	References
availability as a business driver			
service provider - ecosystem availability of validation systems as a matter of trust		1	1
service provider - ecosystem challenges of selective disclosure in audits		1	1
service provider - ecosystem CIRs introducing breaking changes to business models		1	1
service provider - ecosystem CIRs introducing breaking changes to trust service providers		1	1
service provider - ecosystem data availability challenges limiting uptake		1	1
service provider - ecosystem drive to merely adopt EUDIW as identification		1	1
service provider - ecosystem dynamics of ecosystem building		1	1
service provider - ecosystem EUDI adoption being tied to network effects		1	1
service provider - ecosystem eudif requirements making implementation more challenging		1	1
service provider - ecosystem exclusive focus on EUDIW		1	1
service provider - ecosystem fast pace of regulatory developments being pushed to the ecosystem		1	1
service provider - ecosystem government authentic data as a business case enabler		1	1

Name	Description	Files	References
service provider - ecosystem having a regulatory first focus to eidas digital transformation		1	1
service provider - ecosystem importance of government stakeholder in Belgian context		1	1
service provider - ecosystem KYC as a cross sectoral business case		1	1
service provider - ecosystem lack of clear definitions of artifacts to enable more business cases		1	1
service provider - ecosystem lack of common standards for authentic source access		1	1
service provider - ecosystem lack of use cases on delivering business cases		1	1
service provider - ecosystem mastering competencies for ecosystem participation		1	1
service provider - ecosystem national legislation not adjusted for eudif		1	1
service provider - ecosystem perceived benefits for having an overview of the eudif ecosystem		1	1
service provider - ecosystem perception of use case value with eudiw		1	1
service provider - ecosystem PID as the main driver of attribute ecosystem		1	1
service provider - ecosystem PPPs creating facilitating conditions for digital identity adoption		1	1
service provider - ecosystem process requirements defined by law		1	1

Name	Description	Files	References
service provider - ecosystem regulatory requirements challenging small players		1	1
service provider - ecosystem specifics and challenges of law in digital identity transformation		1	1
service provider - ecosystem stringent regulation blocking use cases		1	1
service provider - ecosystem unclear use cases for b2b data sharing		1	1
service provider - ecosystem use cases for EAAs existing outside of EUDIW		1	1
service provider - ecosystem wallet as a use case driver for critical industries		1	1
service provider - ecosystem wallet capability to support multi party transactions missing		1	1
service provider - ecosystem wallet primarily as a business process driver		1	1
service provider - individual usability of eudiw as an ecosystem level challenge		1	1
service provider - individuals individual wallet adoption challenges		1	1
service provider - individuals selective disclosure enabling increased privacy in private sector use cases		1	1
service provider - individuals use difficulty of SSIs for adoption		1	1
service provider - private sector approach to digital transformation to enable business cases		1	1

Name	Description	Files	References
service provider - private sector awareness levels of critical industries		1	1
service provider - private sector data sharing enabling private sector uses cases		1	1
service provider - private sector EAAs enabling private sector relying party use cases with selective disclosure		1	1
service provider - private sector EUDIW adoption strategies		1	1
service provider - private sector hesitant behaviour of critical sector towards the wallet		1	1
service provider - private sector perception of business value with eudiw		1	1
service provider - private sector relying parties companies prioritising process level changes instead of full ecosystem adoption		1	1
service provider - private sector relying parties government authentic data enabling KYC business cases		1	1
service provider - private sector relying parties readiness of private sector relying parties constrained by changes needed in data management		1	1
service provider - private sector relying parties value and revenue models for the wallet		1	1
service provider - private sector relying parties wallet adoption requiring large scale business process and business ecosystem transformation		1	1
service provider - private sector relying parties wallet adoption requiring large		1	1

Name	Description	Files	References
scale transformation for companies			
service provider - private sector relying parties wallet as a KYC use case driver		1	1
service provider - private sector strategies for transformation		1	1
service provider - public sector authentic data service quality as an adoption barrier		1	1
service provider - public sector awareness levels of federal government		1	1
service provider - public sector benefits of wallet adoption for g2c and g2b use cases		1	1
service provider - public sector capability modelling on better program alignment in the Netherlands		1	1
service provider - public sector challenge of technical implementation of policy requirements		1	1
service provider - public sector challenges of co opting each other's services in multi level governance structures in Belgium		1	1
service provider - public sector challenges of enacting attribute validation services in Belgian context		1	1
service provider - public sector challenges of multi level governance of eudif rollout in Belgium		1	1
service provider - public sector challenges of overfocusing on regulation in digital transformation		1	1
service provider - public sector challenges with accessing authentic data		1	1
service provider - public sector change in analogue		1	1

Name	Description	Files	References
modes of thinking around business processes			
service provider - public sector collaboration aspects of eudif rollout in Belgium		1	1
service provider - public sector common governance challenges in the Belgian context		1	1
service provider - public sector complex nature of DPIs in Belgian context		1	1
service provider - public sector data issuing party motivation to inherit trust via collaborations		1	1
service provider - public sector distribution of use cases across b2b and b2g		1	1
service provider - public sector division of responsibilities towards eudif implementation		1	1
service provider - public sector EAAs enabling seamless business processes		1	1
service provider - public sector eudif rollout governance aspects in Belgium		1	1
service provider - public sector governance aspects of authentic sources in Belgian eudif rollout		1	1
service provider - public sector governance aspects of digital identities in Belgium		1	1
service provider - public sector hands on approach to digital transformation		1	1
service provider - public sector immature enterprise architecture practice in Dutch authorities		1	1
service provider - public sector impact of legacy systems on change management		1	1

Name	Description	Files	References
service provider - public sector importance of having the right stakeholders for public sector digital identity adoption		1	1
service provider - public sector importance of multi level collaboration in eudif rollout in Belgium		1	1
service provider - public sector importance of natural to legal person mandates in Belgian context		1	1
service provider - public sector involvement of local governments crucial in Belgian eudif rollout		1	1
service provider - public sector lack of eudif awareness		1	1
service provider - public sector legal requirements being drivers for eidas digital transformation		1	1
service provider - public sector linear progression of digital transformation activities		1	1
service provider - public sector multi party capability can be irrelevant for government use cases		1	1
service provider - public sector non existent certification schemes for new products		1	1
service provider - public sector participation and reliance upon private sector in the EUDI ecosystem		1	1
service provider - public sector perception of lacklustre use case value of the wallet while alternative means exist		1	1
service provider - public sector perception of collaborative rollout of eudif in Belgium		1	1

Name	Description	Files	References
service provider - public sector perception of digital identities primarily private sector use case driven due to frequency of use		1	1
service provider - public sector perception of public sector motivation being compliance driven		1	1
service provider - public sector policy organizations supporting rollout with building blocks		1	1
service provider - public sector previous management experience helping in eudif adoption in the government		1	1
service provider - public sector relying parties process redesign relevancy to wallet adoption		1	1
service provider - public sector relying parties SSIs enabling secure authentication mechanisms		1	1
service provider - public sector reuse of building blocks in the public sector		1	1
service provider - public sector role of government in the eudif ecosystem		1	1
service provider - public sector role of the government in eudif ecosystem		1	1
service provider - public sector service and technical requirements to adopt a vendor solution		1	1
service provider - public sector structure of organization resulting in service complexities in Belgium		1	1
service provider - public sector structures and their effect on services and governance		1	1

Name	Description	Files	References
service provider - public sector unclear requirements to operate authentic sources		1	1
service provider - public sector validation schemes necessary for public sector		1	1
service provider - relying parties antecedents of EUDI adoption		1	1
service provider - relying parties awareness levels of ecosystem participants on eudif		1	1
service provider - relying parties SSIs enabling relying party use cases		1	1
service provider - relying parties wallet adoption antecedents of relying parties		1	1
service provider - service provider development of eID means capabilities with EUDI		1	1
service provider - service provider EAA embedded disclosure policy enabling relying party trust on attribute verification		1	1
service provider - service provider EAAs addressing trust problems of common artefacts		1	1
service provider - service provider EAAs allowing new solutions		1	1
service provider - service provider EAAs enabling data confidentiality		1	1
service provider - service provider EAAs enabling economic value and user friendliness		1	1
service provider - service provider EAAs enabling non-governmental data sharing use cases		1	1
service provider - service provider EAAs enabling trust frameworks for identity attributes		1	1

Name	Description	Files	References
service provider - service provider EUDI introducing new capabilities		1	1
service provider - service provider implementation challenges due to regulation immaturity		1	1
service provider - service provider importance of EAAs for data sharing		1	1
service provider - service provider intermediary use cases enabled by consent mechanisms		1	1
service provider - service provider process of digital transformation		1	1
service provider - service provider qtsp liability in electronic transactions		1	1
service provider - service provider strategy to implement EUDI against technology and dependencies of the ecosystem		1	1
service provider- public sector relying parties wallets effect on government workflows		1	1
slow uptake of eudif in Dutch central government		1	1
small jurisdictions needing support for implementation		1	1
specifics and challenges of law in digital identity transformation		1	1
SSIs enabling secure authentication mechanisms		1	1
stakeholder communication of digital identity means change in local governments		1	1
status of PPP developments around eudiw use in Belgium		1	1
strategies for creating support systems		1	1
strategies for orchestrators		1	1

Name	Description	Files	References
strategies to initiate adoption mechanisms		1	1
strategy to implement EUDI against technology and dependencies of the ecosystem		1	1
structure of organization resulting in service complexities in Belgium		1	1
structures and their effect on services and governance		1	1
technical and legal requirements for wallet providers for procurement		1	1
technical changes needed to support wallet use cases at local governments		1	1
technology adoption modes of public sector		1	1
transparency aspects over issuers		1	1
unclear law		1	1
unclear requirements to operate an authentic source		1	1
unclear use cases for b2b data sharing		1	1
usability of eudiw as an ecosystem level challenge		1	1
Use cases for EAAs existing outside of the EUDIW		1	1
use difficulty for SSI adoption on the public sector		1	1
use of authentic data enabling relying party use cases		1	1
use of trust components part of the organizational value proposition		1	1
utilizing citizen trust for local levels for legitimacy building		1	1
validation schemes necessary for public sector		1	1

Name	Description	Files	References
value and revenue models of wallet use in private sector		1	1
value propositions of wallet choice		1	1
wallet adoption antecedents of relying parties		1	1
wallet adoption motivation for internal processes use cases in local government		1	1
wallet adoption requiring extensive transformation for companies		1	1
wallet adoption requiring large scale business transformation		1	1
wallet as a driver for private sector use cases in critical industries		1	1
wallet as a use case driver in KYC		1	1
wallet capabilities changing usual service delivery processes		1	1
wallet capabilities enabling value for public relying parties		1	1
wallet capabilities supporting data quality in processes		1	1
wallet capability to support multi part transactions missing		1	1
wallet operation challenged by business models for authentic data providers		1	1
wallet primarily as a business process driver		1	1
wallet provider - ecosystem eudif getting rolled out in active engagement to mitigate national law alignment problems		1	1
wallet provider - ecosystem unclear law		1	1
wallet provider - public sector challenges of fast changing environment on public procurement		1	1

Name	Description	Files	References
wallet provider - public sector challenges of open code approach		1	1
wallet provider - public sector decentralization of procurement knowledge		1	1
wallet provider - public sector funding and procurement processes exhibit gaps		1	1
wallet provider - public sector mechanisms to engage wallet providers early on		1	1
wallet provider - public sector past engagements and awareness of public sector around eudif		1	1
wallet provider - public sector public sector governance on setting out ecosystems		1	1
wallet provider - public sector public sector on procurement governance		1	1
wallet provider - public sector technical and legal requirements for wallet providers for procurement		1	1
wallet provider - public sector wallet providers experience on collaborating with the public sector		1	1
wallet providers - public sector practicalities of dealing with national law		1	1
wallet providers experience on collaborating with the public sector		1	1

Table 8 Codebook Author's elaboration

I Intermediary governance model artifact

This governance model artifact was developed solely by the author prior to evaluation rounds as an intermediary model for presenting design objectives from the literature prior to their evaluation and as a result was not presented in the results of this thesis.

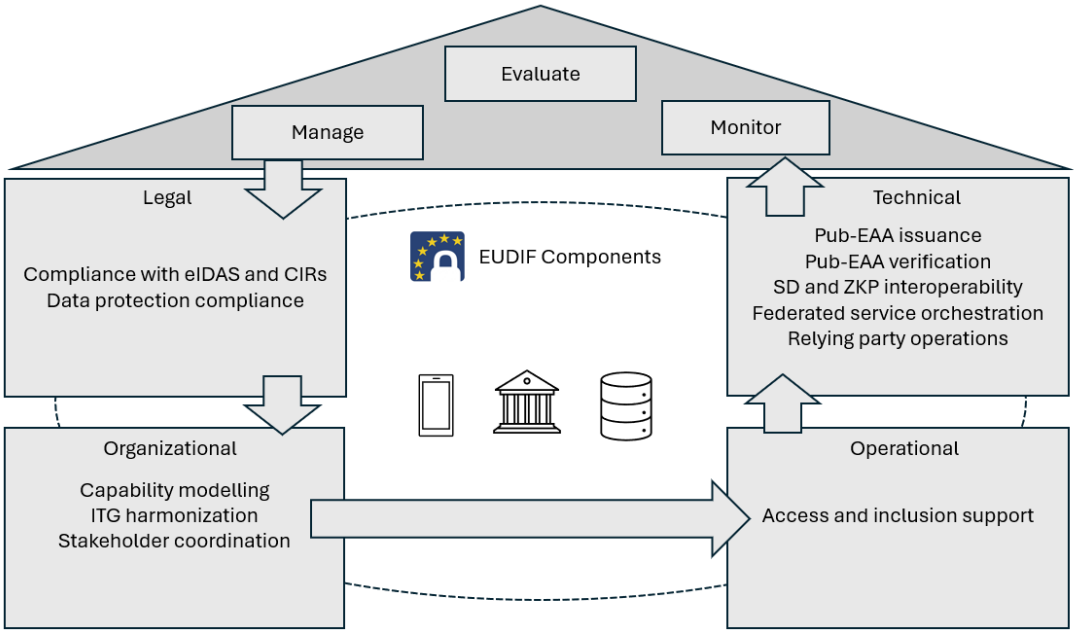

Figure 16 Intermediary governance model artifact Author's elaboration

J Selection of Open Agile Architecture (OAA by Open Group) blocks towards governance model artifact modelling contexts.

Table 9 Selection of O-AA building blocks Author's elaboration

Selected OAA reference building blocks	Building block	Modelling context
1	4.2-6	Model wireframe development
2	5.5-8	Service design, process redesign
3	7.1-11	Organizational context, management context
4	10.1-19	Hierarchy of modelling components
5	10.3-21	Hierarchy of modelling components
6	15-35	Service design
7	16.1.3-36	Process redesign, use case definition
8	16.2-38	Process redesign, use case definition
9	17-44	Management context, organizational repository, process redesign, use case definition

K First iteration of the governance model artifact

The artifact below has been modeled in accordance with the evaluated design objectives derived from the first phase of expert interviews.

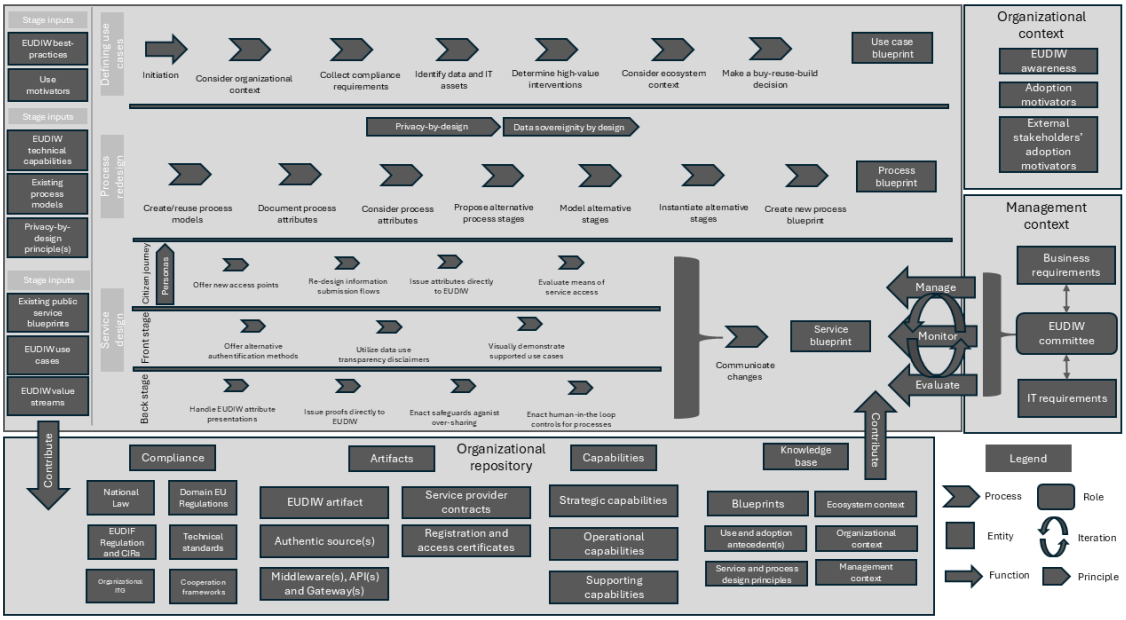

Figure 17 First iteration of the governance model artifact Author's elaboration

L Mapping of design components, entities and features to our research knowledge base in the second iteration of the governance model artifact.

The table below enumerates all design components, entities and features present in the final iteration of the governance model artifact. Each enumeration is linked to a corresponding interview and/or a literature entry. Thus, presenting justifications to each design element that has been incorporated. Table entries can be identified via the numbering scheme presented on the final model iteration.

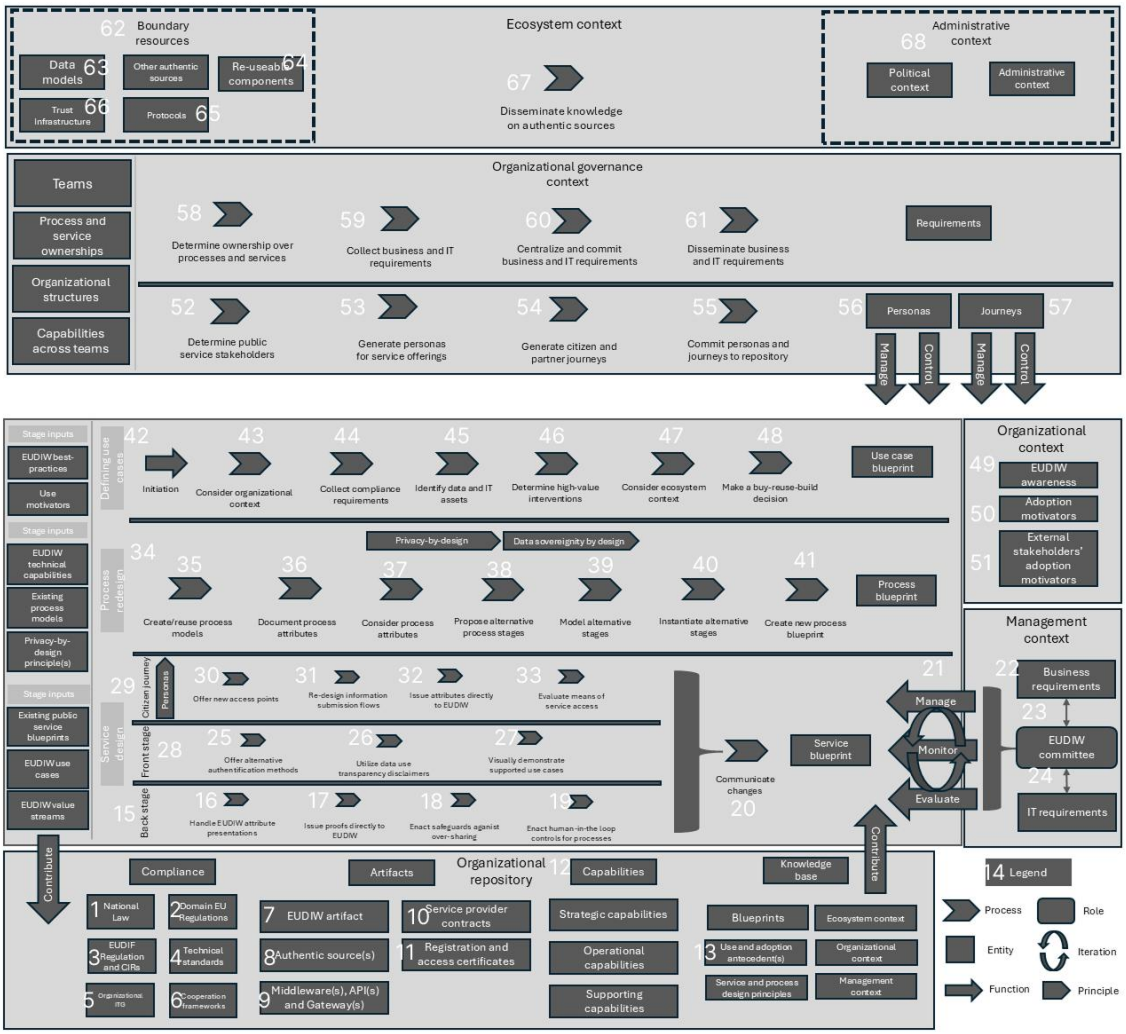

Figure 18 Design element mapping of the second iteration model artifact Author's elaboration

Design element	Supporting interview(s)	Supporting literature(s)	Supporting design objective(s)
1	6, 10, 14, 17	(Kolehmainen, 2021)	DO3
2	10, 23	(Kolehmainen, 2021)	DO3
3	8, 10, 14, 17	(European Commission, 2024), (European Commission, 2025)	DO3
4	4, 8, 9, 21	(Kolehmainen, 2021)	DO3
5	14	(Kolehmainen, 2021)	DO3
6	21	(Kolehmainen, 2021)	DO3

7	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 25, 26, 27, 28	(European Commission, 2024)	DO7
8	4, 8, 5, 9, 12, 15, 21	(European Commission, 2024)	DO7
9	14, 25, 4, 5, 8, 15		DO7
10	6, 5, 4		DO7
11	9	(European Commission, 2024), (European Commission, 2025)	DO7
12	14, 19, 21		DO7
13	2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 15, 18, 22		DO7
14			High-level DO
15		(Group, 2025)	DO6
16	18		DO6
17	18, 14		DO6
18	24, 14, 26		DO6
19	28, 27		DO6
20	14, 18, 20, 15, 17		DO6
21	10, 14, 3		DO5
22	14, 3, 4, 6, 8	(Kölbel et al., 2022)	DO5
23	10, 14	(Kölbel et al., 2022)	DO5
24	14, 3, 4, 6, 8	(Kölbel et al., 2022)	DO5
25	28, 26		DO6
26	18	(Korir et al., 2022)	DO6
27	18		DO6
28		(Group, 2025)	DO6
29		(Group, 2025)	DO6

30	28, 26, 18		DO6
31	14, 18	(Korir et al., 2022)	DO6
32	14, 1, 7		DO6
33	26, 28		DO6
34		(Group, 2025)	DO4
35	10, 11, 12, 14, 18, 21, 22	(Da Silva Carvalho et al., 2023), (van Rest et al., 2014b)	DO4, DO1
36		(Da Silva Carvalho et al., 2023), (van Rest et al., 2014b)	DO4, DO1
37		(Da Silva Carvalho et al., 2023), (van Rest et al., 2014b)	DO4, DO1
38		(Da Silva Carvalho et al., 2023), (van Rest et al., 2014b)	DO4, DO1
39		(Da Silva Carvalho et al., 2023), (van Rest et al., 2014b)	DO4, DO1
40		(Da Silva Carvalho et al., 2023), (van Rest et al., 2014b)	DO4, DO1
41		(Da Silva Carvalho et al., 2023), (van Rest et al., 2014b)	DO4, DO1
42	22, 1, 2, 3, 4, 8, 9, 10, 12, 14, 15, 21	(Liesbrock & Sneiders, 2024)	DO2
43		(Liesbrock & Sneiders, 2024)	DO2
44		(Liesbrock & Sneiders, 2024)	DO2
45		(Liesbrock & Sneiders, 2024)	DO2

46		(Liesbrock & Sneiders, 2024)	DO2
47		(Liesbrock & Sneiders, 2024)	DO2
48		(Liesbrock & Sneiders, 2024)	DO2
49	7, 8		DO5
50	2, 3, 4, 5, 8, 10, 11, 12, 14, 15, 16, 18, 22		DO5
51	22, 18, 15, 14, 11, 8, 2		DO5
52	14, 18, 28,		DO6
53			DO6
54			DO6
55			DO6
56			DO6
57			DO6
58	14, 24, 27		DO5
59			DO5
60			DO5
61			DO5
62	14, 4, 9, 15		DO5
63			DO5
64			DO5
65			DO5
66			DO5
67	12	(Kubach et al., 2020)	DO5
68	17, 10, 8, 15		DO5

Table 10 Design element mapping table of the second iteration of model artifact Author's elaboration

M Table of design changes towards the first iteration of the governance model artifact.

This table depicts elements of ascertained design changes to be applied toward generating the second iteration of the artifact. Summarized design changes represent authors' analysis of expert's perceptions and subsequent feedback of the first iteration of the artifact. Design changes are formulated in accordance with existing design objectives to ensure their fit in the modelling context.

Design change	Summary of change	Supported design objective(s)	Supporting interview(s)
1	Depict a workflow for collecting business and IT requirements for process and service redesign	DO4, DO6, DO2	14
2	Model ecosystem-level entities	DO5	12, 15
3	Model public service, client-facing requirements	DO2, DO6	14

Table 11 Table of design changes towards the first iteration of the artifact Author's elaboration

N Second and final iteration of the governance model artifact

This artifact has been generated, using the first iteration, situated at Annex K, and incorporating the 3 design changes, formulated as a result of 10 expert interviews. All artifact features and elements were kept from the first iteration as we have not received feedback related to their unsuitability. Three additional main stages were mapped, called organizational governance context (1), (2) and ecosystem context. The artifact below constitutes the second and final iteration of the governance model in the context of this thesis.

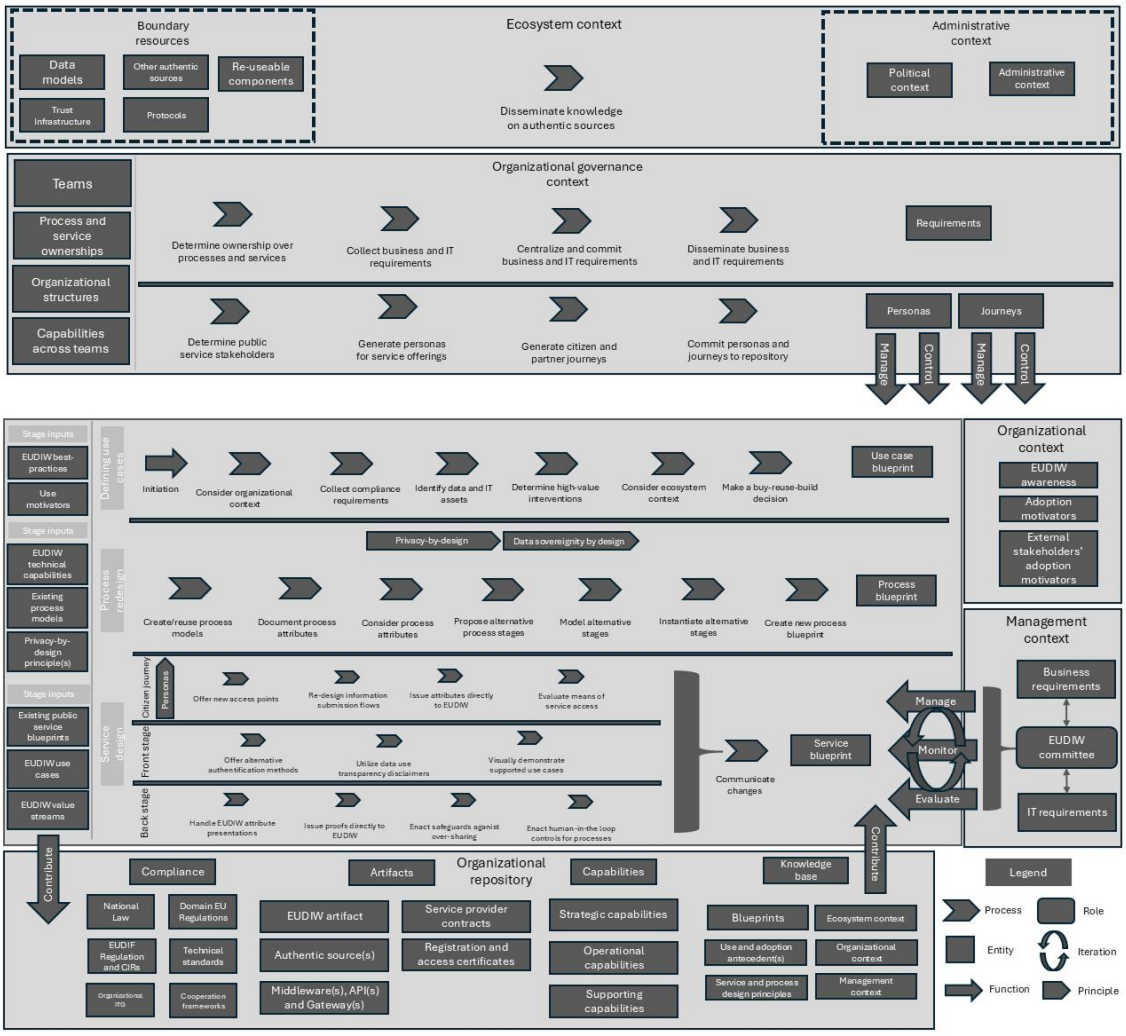

Figure 19 Second iteration of the governance model artifact Author's elaboration

O Core and auxiliary design principles and ecosystem goals of the EUDIF ecosystem as presented in ARF

The principles and goals presented in the table below form the basis of our modeling approach from a public value creation perspective for public sector organizations. Throughout this thesis, we aim to present use-cases, identify methods, structures, hierarchies and relational dynamics applicable to organizational contexts in order to inform the governance of EUDIF elements in a way that results in the operationalization and integration of these principles and goals in public sector processes, service design and operations.

Table 12 Design principles and ecosystem goals of the EUDIF ecosystem Adapted from (European Commission, 2025)

Core design principles	Auxiliary design principles	Ecosystem goals
User centricity	User friendliness Full data control Transaction transparency	Fostering trust Encouraging adoption
Interoperability	Use of standardised protocols Seamless credential verification Ecosystem harmonization by interoperable design	Innovation, competition and collaboration Universal acceptance
Privacy-by-design	Protection of user data Data minimisation Selective disclosure Transparency	Fostering trust Protecting fundamental rights
Security-by-design	Security by architectural design Data compartmentalization Secure coding practices	Ecosystem resilience Fostering trust and confidence in the ecosystem

P Classification of public value creation mechanisms supported by the governance model artifact

The classification table below has been constructed to link conceptual dimensions of public value creation in digital government systems with the features of our artifact. We use the conceptual scheme offered by (Twizeyimana & Andersson, 2019) in construction of the table. We suggest that via the adoption of our model artifact, public sector organizations can further the identified modes of public value creation.

Artifact feature	Description of artifact feature	Supported public value creation mechanism
1	Organizational repository context	Improved public services, improved administrative efficiency

2	Service design stage	Improved public services, improved administrative efficiency, improved trust and confidence in government
3	Process design stage	Improved trust and confidence in government, improved public services, improved administrative efficiency
4	Use case definition stage	Improved trust and confidence in government, improved administrative efficiency
5	Organizational governance context	Improved ethical behavior and professionalism
6	Ecosystem context	Improved ethical behavior and professionalism, Open government (OG) capabilities

Table 13 Classification of public value creation mechanisms supported by the governance model artifact. Author's elaboration

Q Evaluation of high-level design objectives of the governance model artifact

Design objective		Success Requirements		
		Problem Level & Stakeholders	**Goal Achievement**	**Artifact Trait**
1	Depict organizational context in sufficient complexity.	Organizations	Partially supported	Represents, roles, relations, and activities for EUDIF governance
2	Offer compatibility with common ITG frameworks in the public sector.	Organizations	Fully supported	-Modeled according to O-AA specification
3	Offer compatibility with standard modelling tools and extensions.	Organizations	Fully supported	Capable of supporting ArchiMate modelling due to shared O-AA Architecture
4	Offer accountability and auditability capabilities.	Organizations	Partially supported	Offers a simple, bird's eye view of EUDIF governance controls.
5	Define relational structures and roles around the use of IT	Organizations	Fully supported	Defines controls and activities for governing EUDIWs in organizations

Table 14 Evaluation of the high-level design objectives of the governance model artifact Author's elaboration

Declaration of Authorship

I hereby declare that, to the best of my knowledge and belief, this Master Thesis titled "Digital Credentials in your Wallet: A Design Knowledge approach to European Digital Identity Framework governance for public sector organizations" is my own work. I confirm that each significant contribution to and quotation in this thesis that originates from the work or works of others is indicated by proper use of citation and references.

Leuven, 16 June 2025

Yiğit Aşkan

Consent Form

for the use of plagiarism detection software to check my thesis

Name: Aşkan
Given Name: Yiğit
Student number: 552632
Course of Study: Public Sector Innovation and eGovernance
Address: Schlossplatz 2, 48149 Münster
Title of the thesis: Digital Credentials in your Wallet: A Design Knowledge approach to European Digital Identity Framework governance for public sector organizations

What is plagiarism? Plagiarism is defined as submitting someone else's work or ideas as your own without a complete indication of the source. It is hereby irrelevant whether the work of others is copied word by word without acknowledgment of the source, text structures (e.g. line of argumentation or outline) are borrowed or texts are translated from a foreign language.

Use of plagiarism detection software. The examination office uses plagiarism software to check each submitted bachelor and master thesis for plagiarism. For that purpose the thesis is electronically forwarded to a software service provider where the software checks for potential matches between the submitted work and work from other sources. For future comparisons with other theses, your thesis will be permanently stored in a database. Only the School of Business and Economics of the University of Münster is allowed to access your stored thesis. The student agrees that his or her thesis may be stored and reproduced only for the purpose of plagiarism assessment. The first examiner of the thesis will be advised on the outcome of the plagiarism assessment.

Sanctions. Each case of plagiarism constitutes an attempt to deceive in terms of the examination regulations and will lead to the thesis being graded as "failed". This will be communicated to the examination office where your case will be documented. In the event of a serious case of deception the examinee can be generally excluded from any further examination. This can lead to the exmatriculation of the student. Even after completion of the examination procedure and graduation from university, plagiarism can result in a withdrawal of the awarded academic degree.

I confirm that I have read and understood the information in this document. I agree to the outlined procedure for plagiarism assessment and potential sanctioning.

Leuven, 16 June 2025

Yiğit Aşkan