Alper Tanrıverdi

The Road to EU-Wide Digital Identity Wallet Adoption: Insights from Estonia and Belgium's EUDI Wallet Implementation

Master Thesis

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

Supervisor: Prof. dr. ir. Joep Crompvoets

Presented by: Alper Tanrıverdi
Rue François Bossaerts 49
1030 Brussels
+32 490 21 76 60
alper.tanriverdi@student.kuleuven.be

Date of Submission: 2025-06-02

Content

Figures

Tables

Abbreviations

ANT	Actor-Network Theory
ARF	Architecture and Reference Framework
CCB	Cybersecurity Centre Belgium
CP	Controlling Party
DTC	Digital Travel Credential
DSM	Digital Single Market
EAA	Electronic Attestation of Attributes
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication and Trust Services (Regulation)
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUDI	European Digital Identity
EUDIW	European Digital Identity Wallet
ESSIF	European Self-Sovereign Identity Framework
FPS	Federal Public Service
GDPR	General Data Protection Regulation
IdM	Identity Management
IdP	Identity Provider
PESTEL	Political, Economic, Social, Technological, Environmental, and Legal (analysis framework)
PID	Personal Identity Dataset
PKI	Public Key Infrastructure
QEAA	Qualified Electronic Attestation of Attributes

RIA	Regulatory Impact Assessment
SDGR	Single Digital Gateway Regulation
SLR	Systematic Literature Review
SP	Service Provider
SSI	Self-Sovereign Identity

Abstract

The European Digital Identity Wallet (EUDIW) emerges as a key instrument to enable secure cross-border digital interactions for citizens and businesses. National implementation strategies diverge due to differences in governance structures, digital maturity, and stakeholder coordination. This thesis investigates the factors shaping EUDIW implementation in Estonia and Belgium, two early adopters with contrasting administrative models and digital ecosystems. Applying a theoretical framework grounded in Actor-Network Theory (ANT) and PESTEL analysis, the research explores how human and non-human actors, along with broader external influences, structure national approaches to the wallet. Through a qualitative multi-method design combining semi-structured expert interviews and document analysis, the study identifies key stakeholder roles, contextual drivers, and barriers in each country. The results show that Estonia pursues a centralized, procurement-based implementation led by the Information System Authority (RIA), whereas Belgium adopts a more fragmented, state-led strategy involving multiple federal and regional actors. Both countries encounter common implementation hurdles, including missing EU-level guidelines, certification delays, and limited public understanding of the wallet's added value. These findings illustrate that the EUDIW rollout is not merely a technical deployment, but a deeply socio-political process that depends on network alignment, institutional readiness, and citizen engagement. By comparing the Estonian and Belgian cases, this research provides empirically grounded insights into EUDIW adoption dynamics. It contributes to existing literature by offering one of the first country-specific analyses of EUDIW implementation as well as provides practical insights for EU institutions and Member States to design adaptive, inclusive, and harmonized strategies.

1 From eIDAS to European Digital Identity Wallet (EUDIW)

The Single Market is a cornerstone of European Union (EU) integration, ensuring that services, alongside goods, capital, and people, can move freely across the Union as though within a single country. This freedom of movement now increasingly depends on the accessibility of digital services, which play a vital role in economic and social interactions.

Access to digital services, however, is not just a question of availability or demand. It also requires secure and efficient digital identification mechanisms for individuals, companies, and organizations. The European Digital Identity Wallets (EUDIW) emerge as a response to this challenge, forming the centerpiece of the EU's new approach under the European Digital Identity (EUDI) Regulation. This Regulation, adopted in 2024, aims to establish a universal, secure, and user-centered digital identity system that is interoperable across Member States (European Commission, 2025).

While the Regulation establishing the European Digital Identity Framework has entered into force (Regulation (EU) 2024/1183, 2024); the five Implementing Acts setting the rules for the core functionalities, uniform implementation of the wallet across Europe and certification of the eID Wallets have been adopted (European Commission, 2024); and the EU Digital Identity Toolbox serving as the technical backbone of all future EU Digital Identity wallets, ensuring their safety, interoperability, and user friendliness has been published (European Commission, 2023b, 2023a); a well-functioning ecosystem in which the key stakeholders closely collaborate still needs to be built for a successful implementation of the European Digital Identity Wallets within the Member States (European Digital Identity Wallet, 2025).

This research examines the implementation of the European Digital Identity Wallet in Estonia and Belgium, focusing on the key factors shaping this process, including barriers, drivers, and stakeholder involvement. Additionally, it explores the lessons that can be drawn from these cases to inform the broader European context.

In order to contextualize this research, first, it is important to define what is meant by digital identity. In offline settings, identification typically involves presenting physical credentials that confirm personal attributes such as name, date of birth, or nationality. In digital contexts, these attributes are represented electronically and can be used to authenticate users for online services. Secure digital identity is therefore foundational to accessing eGovernment services, financial platforms, healthcare systems, and educational institutions. According to Eurostat (2024), in 2024 over 70 percent of individuals in the

EU used digital public services. Many of these rely on electronic identification mechanisms.

While some Member States already operate robust national eID systems, these often lack interoperability beyond national borders. This mismatch hinders the EU's broader vision of a truly integrated digital space. The eIDAS Regulation, originally adopted in 2014, attempted to address this by mandating the mutual recognition of national eIDs across Member States (Regulation (EU) 910/2014, 2014). It created a federated trust framework in which each country maintains its own infrastructure while connecting to others through standardized eIDAS nodes.

Despite this achievement, briefing on the Revision of the eIDAS Regulation Findings published by the European Parliament (2022) highlighted several shortcomings of the existing eIDAS regulation. First, it failed to meet the growing demand from public and private services for trusted identification and digital attribute exchange. Second, it did not align with user expectations for seamless and reliable cross-border identification and attribute sharing. Third, existing digital identity solutions fell short in addressing evolving concerns over data control and security. Lastly, in the realm of trust services, the regulation's limited scope and the absence of a level playing field across the EU hindered the development of a unified internal market. These limitations formed the rationale for revising eIDAS and introducing the European Digital Identity Wallet under eIDAS 2.0 (EUR-Lex, 2021; Lukkien et al., 2023).

The wallet is envisioned as a mobile application through which users can store and manage a wide range of credentials, from driving licences to academic diplomas. It is designed to provide selective disclosure, allowing individuals to share only the information necessary for a given transaction. Crucially, the new approach shifts control over data to the user, aligning with evolving expectations around privacy, sovereignty, and transparency (European Commission, 2025; Regulation (EU) 2024/1183, 2024).

However, there is limited academic consensus on whether this shift toward a user-controlled identity model is feasible or desirable in the long term. Some scholars question whether federated or even self-sovereign identity systems can ensure accountability across jurisdictions, or whether centralized models offer better governance (Abraham et al., 2021; Landrigan et al., 2023; Podgorelec et al., 2022; Zwattendorfer et al., 2014). Others emphasize the risks of fragmentation and uneven implementation across Member States (Degen & Teubner, 2024; Khayretdinova et al., 2022; Kostic, 2024; Lukkien et al., 2023). These debates remain underdeveloped and require further empirical grounding.

1.1 Problem Definition and Research Gap

The development and implementation of European Digital Identity Wallets are shaped by various factors including the interests and capacities of a wide range of actors. According to the European Union Agency for Cybersecurity (ENISA, 2024), from the perspective of citizens, digital identity wallets offer greater ease of access and potentially stronger privacy protections. For governments, digital identity wallets simplify administrative processes, protect personal data, and enhance access to cross-border services while improving security and fraud prevention. For relying parties, such as businesses and service providers including financial institutions, healthcare providers, and telecom companies, the wallets reduce authentication costs, enhance security and privacy, and mitigate dependence on competing private platforms. These factors underscore the necessity of a well-structured and interoperable digital identity ecosystem within the EU.

For well-functioning EUDIWs, a thriving EU Digital Identity Wallet ecosystem in which digital IDs and digital documents can be readily issued and verified should be established (European Digital Identity Wallet, 2025). Implementation therefore requires coordinated action among wallet providers who develop technological solutions, credential issuers who supply verifiable data, and relying parties who integrate the wallet into service provision. Each of these actors operates within different incentive structures, legal mandates, and technical constraints.

To test and develop the wallet's functionalities, the European Commission launched four large-scale pilot projects. Each focus on different use-cases, ranging from digital payments and travel credentials to education and healthcare services. The NOBID Consortium (2022), comprising Nordic and Baltic countries alongside Italy and Germany, is developing a large-scale pilot focusing on payments, enabling secure transactions within the EUDIW framework. Potential (2023) explores the use of a secure digital ID for various applications, including mobile driving licenses, access to government services, banking, healthcare, contract signing, and SIM registration. The EWC (2023) project seeks to harness EUDIW capabilities for Digital Travel Credentials (DTCs), leveraging the Reference Wallet Application to support payments, travel, and organizational identity verification. Lastly, DC4EU (2025) integrates advanced digital services across Europe, with a specific focus on education and social security, aiming to establish a cross-border trust framework for seamless interoperability.

Building on these broader European initiatives, individual Member States have taken distinct approaches to develop and implement their EUDIWs. Estonia and Belgium stand out as the pioneers of the EUDIW adoption, each leveraging their existing digital infrastructure to shape their national strategies within the evolving EU framework

(Cybernetica, 2024; Walker, 2024). According to a news article published by The Brussels Times (Walker, 2024), Belgium is among the first EU Member States to launch a European Digital Identity Wallet.

Belgium, with its MyGov.be application, serves as a central platform integrating various government services. Given Belgium's complex administrative model, the digital wallet aims to streamline interactions between citizens and public authorities. MyGov.be (2024) currently provides access to the Federal Government's secure electronic mailbox (eBox), used by millions of citizens, and functions as an electronic repository for official documents such as birth and marriage certificates. The initial 1.0 version of the wallet includes a limited set of features, such as access to COVID-19 vaccination certificates and the ISI+ card for individuals covered by Belgian social security. Additionally, MyGov.be enables citizens to request certificates via a virtual counter and authenticate their identity online, with future upgrades expected to introduce digital signatures and document-sharing functionalities.

Estonia, on the other hand, is building on its long-standing leadership in digital governance, seeking to integrate the wallet into an already mature digital identity ecosystem (e-Estonia, 2024). The Estonian Information System Authority (RIA) oversees the development of Estonia's digital wallet, ensuring its compatibility with the existing electronic identity infrastructure (Information System Authority, 2024). Since the adoption of eIDAS 2.0, extensive analyses have been conducted on the wallet's technical architecture, including the feasibility of integrating various digital certificates, such as a mobile driving license (Cybernetica, 2024).

Despite these developments, the implementation of EUDIWs continues to face significant barriers. Several of these challenges have been identified by Lukkien et al. (2023), ENISA (2024), and Degen and Teubner (2024). One of the key challenges is the absence of a unified EU-wide certification scheme, which has necessitated reliance on national certification frameworks as temporary solutions. Achieving harmonization across these national schemes is critical for ensuring the security, trust, and interoperability of EUDIWs. Additionally, the involvement of numerous stakeholders, combined with misalignment between EU-level legislation and national policies, adds complexity to coordination and cross-sectoral collaboration. Technical and socio-technical issues such as the lack of standardization, inconsistencies in data formats, and difficulties in integrating with existing digital identity infrastructures further hinder widespread adoption. Economic challenges, including high initial investment requirements, disruptions to established business models, and diminished control over digital assets, have also created resistance, particularly among private sector actors. Furthermore,

concerns related to digital inclusion persist, as varying levels of digital literacy and readiness across different demographic groups may limit the accessibility and usability of EUDIWs. Legal uncertainty, especially the lack of regulatory harmonization and clarity, compounds these issues and adds to the complexity of implementation.

These challenges are especially significant given the complex nature of the EUDIWs ecosystem. This ecosystem comprises a network of autonomous public and private entities that are responsible for issuing, managing, and verifying digital identity data originating from various sources and trust levels (Degen & Teubner, 2024). Operating under a model of shared governance, the ecosystem is designed to generate collaborative value for users, governments, and businesses. However, the successful adoption of EUDIWs requires the integration of diverse stakeholder perspectives, and managing this complexity poses a considerable challenge for Member States.

The nascent state of academic literature on EUDIW compounds these implementation challenges. In their study of EUDIW implementation barriers in the Netherlands, Lukkien et al. (2023) emphasize the abundance of obstacles and the absence of clear guidance for the design, development, and deployment of digital identity wallets within a public-private ecosystem. A Scopus database search conducted in January 2023 for academic literature containing the term “Digital Identity Wallet” in the title, keywords, or abstract yielded only ten results. Most of these studies focus predominantly on technological or security aspects, rather than addressing the broader social and organizational dimensions. This highlights a significant gap in the academic discourse, particularly with respect to the socio-technical challenges associated with the development and launch of digital identity wallets in complex, collaborative environments.

1.2 Case Selection, Research Goal and Research Questions

Estonia and Belgium are purposefully selected as case studies due to their contrasting yet complementary roles in the European Digital Identity Wallet landscape. Estonia is internationally recognized as a pioneer in digital government, offering a mature and widely adopted electronic identity system that has been operational for over two decades (Lips et al., 2023). Its digital infrastructure is underpinned by the X-Road framework, which enables secure and efficient data exchange between public and private organizations. While the governance of Estonia’s eID ecosystem remains centrally coordinated by state institutions such as the Estonian Information System Authority (RIA), the technical architecture is decentralized in the sense that data is not stored in a single repository but distributed across autonomous databases owned by different entities (Mander et al., 2023). This federated structure supports interoperability, resilience, and

scalability making Estonia a relevant benchmark for advanced integration of EUDIW functionalities.

In contrast, Belgium presents a compelling case of early adoption within a more fragmented administrative model, where different levels of government, namely federal, regional, and local coexist (Brans et al., 2006; Mariën & Van Audenhove, 2010). This complexity offers valuable insights into how a European Digital Identity Wallet can be operationalized in less centralized governance settings while navigating inter-institutional coordination challenges.

Importantly, while both countries are recognized as front runners in EUDIW development, there is a notable absence of country-specific case studies in academic literature. Most existing studies tend to focus on the European framework at large or explore only the technological aspects of digital identity (Lukkien et al., 2023). By conducting in-depth analyses of Estonia and Belgium, this research addresses a critical gap in the literature and offers empirically grounded insights that can inform implementation strategies in other EU Member States with similar digital maturity or administrative complexity.

The primary objective of this study is to examine the factors shaping the implementation strategies of the European Digital Identity Wallet in Estonia and Belgium. By focusing on the roles, interests, and challenges faced by key stakeholders, the research aims to uncover how these factors shape national implementation strategies and the overall effectiveness of EUDIW deployment efforts. Through a comparative analysis of both countries, this research not only explores the drivers and barriers encountered at the national level but also identifies strategic approaches and practices that may contribute to a more harmonized, inclusive, and scalable digital identity framework across the European Union.

In light of this, the research aims to address the question ***"What are the key factors shaping the implementation strategies of the European Digital Identity Wallet (EUDIW) in Estonia and Belgium, and how can these insights inform a cohesive EU-wide approach?"***.

Answering this question requires a comprehensive understanding of the stakeholders involved, the challenges and opportunities they face, and the strategic approaches adopted by Estonia and Belgium. To provide a thorough answer to the main research question, the following sub-questions will be addressed:

1. Who are the key stakeholders in Estonia and Belgium involved in the adoption and implementation of the EUDIW, and what are their roles, interests, and objectives?

2. What are the drivers and barriers for stakeholders in EUDIW implementation?

3. How do Estonia's and Belgium's EUDIW implementation strategies differ, and what lessons can they offer for the broader EU rollout?

This thesis is structured into seven chapters. Following the introduction in Chapter 1, which outlines the research problem, objectives, and case selection, Chapter 2 presents a comprehensive literature review on digital identity, the evolution of identity management models, and the regulatory context of eIDAS and the European Digital Identity Wallet. Chapter 3 introduces the theoretical framework, combining Actor-Network Theory (ANT) and PESTEL analysis, and defines the key concepts used throughout the study. Chapter 4 details the research methodology, including the multi-method approach of document analysis and expert interviews. Chapter 5 presents the empirical findings from the Estonian and Belgian cases, structured around stakeholder ecosystems, drivers and barriers, and national implementation strategies. Chapter 6 offers a comparative discussion of the findings, identifying cross-cutting patterns and key lessons for EU-wide implementation. Finally, Chapter 7 concludes the thesis by summarizing the main insights, discussing limitations, and suggesting directions for future research.

2 Literature Review

The following chapter provides an overview of the academic literature relevant to this research, which investigates the European Digital Identity Wallet (EUDIW) implementation in Estonia and Belgium. The literature review serves a dual purpose. First, providing a comprehensive research background necessary to understand the development and implementation of digital identity wallets in Europe. Second, establishing the foundation for data collection and analysis.

To address the main research question "What are the key factors shaping the implementation strategies of the European Digital Identity Wallet in Estonia and Belgium, and how can these insights inform a cohesive EU-wide approach?" and its sub-questions, the literature review was conducted iteratively and structured using a funnel approach, beginning with general theoretical and conceptual foundations and progressively narrowing to the specific focus of the study. This method allows for a contextualized understanding of the EUDIW by first establishing key concepts such as personal and digital identity, then exploring the evolution of digital identity management models and national eID systems, followed by an in-depth review of the eIDAS and eIDAS 2.0 regulations. The second part of the chapter turns to literature on the foundations and evolution of digital identity wallets, the functional and technical architecture of the EUDIW, and research addressing the stakeholders involved, the main drivers and barriers, and identified use cases.

By following this structure, the chapter outlines what is already known and discussed in academic research, identifies gaps, and positions this study within the broader discussion on digital identity and its implementation across EU member states.

2.1 Personal Identity and Digital Identity

2.1.1 Personal Identity

Identity is widely recognized as both a personal and social construct, shaped by interpersonal contexts as well as environmental factors. It has long been a central topic across various disciplines such as psychology, sociology, and philosophy. In the field of social sciences, academic debate often focuses on the interplay between two primary forms of identity, namely, personal identity and social identity (Carr, 2021; Giddens, 1991; Gur & Mathias, 2021; Swann et al., 2009).

Gur and Mathias (2021) define personal identity as an individual's self-conception formed through unique experiences, memories, and orientations. These attributes

distinguish one person from another across various contexts. In contrast, social identity refers to a person's sense of self that is derived from membership in social groups. Giddens (1991) emphasizes that identity is constructed through language and social norms, making it inherently dynamic and context dependent. Thus, individuals have multiple identities originating from their roles and performances in society. In other words, the definition of who someone is complex and multifaceted, given their multiple and diverging roles and social group membership such as profession, gender, ethnicity, religion, birthplace, role within the home (Manzi & Benet-Martinez, 2022).

Beyond psychological and sociological dimensions, identity also has administrative and functional implications. Carr (2021) critiques the limited view of identity as merely a "core self" or affiliation to social environment. Prusa (2015) argues that identification of citizens via state-issued paper based, or electronic documents such as passports and ID cards is a foundational activity for public administrations globally. These identity documents serve as the means by which individuals verify their identity in both public and private institutional contexts, including banks, healthcare providers, and government offices.

2.1.2 Digital Identity

The digital transformation of public administration has redefined how identity is constructed, managed, and verified. Tan and Crompvoets (2022) explain that the radical transformation of public administration through the adoption of digital technologies is not a new phenomenon. Starting from the first era of digital governance through the utilization of computerization and the Internet at private and public domains, governments attained new capabilities and tools to collect and disseminate information. On the other hand, from the demand side, Scupola and Mergel (2022) note that citizens increasingly expect seamless digital interaction with public institutions. Hence, ICT use in governments have changed how services are designed, delivered, and accessed (Cordella et al., 2018; De Jong et al., 2019).

This overarching digital transformation attempts in the public administration operations, has re-centralized service delivery mechanisms that were previously dispersed across various public and private actors (Dunleavy, 2005). In this context, Prusa (2015) argues that successful and efficient eGovernment requires electronic identification and authentication system. As the information society develops, the need for identification shifts more and more into the Internet realm. Hence, the need to verify identity becomes just as important in the digital realm as in the physical world.

Landrigan et al. (2023) conceptualize digital identity as having two primary functions. First, it serves as a digital representation of personal identity, enabling individuals to enact multiple roles with greater clarity and separation in the virtual domain. Second, and more critically, digital identity functions transactionally. This means it facilitates interactions by providing the necessary information to access specific services, such as healthcare, education, and taxation. These transactions rely on unique digital identifiers to authenticate individuals accurately.

According to Degen and Teubner (2024), digital identity encompasses credentials and attributes that define an individual's relationships with other entities. This structure forms a “root of trust” that allows public and private organizations to recognize and accept digital claims to identity. The ability to prove one’s identity securely online brings identity management (IdM) systems into central focus.

IdM systems regulate user access to digital resources and are a key infrastructure for ensuring secure digital transactions. These systems have been extensively studied across domains such as eGovernment, eBusiness, and eHealth (Landrigan et al., 2023; Podgorelec et al., 2022; Zwattendorfer et al., 2014). As early as the 2000s, governments began to standardize digital signatures and enable frameworks such as public key infrastructures. As Podgorelec et al. (2022) highlight, diverse IdM models have since emerged, varying by governance structure, technological design, and sectoral application.

2.2 Evolution of Digital Identity Management Models

Landrigan et al. (2023) argue that the evolution of digital identity theory and practice provides important insights into the dynamic relationship between digital service delivery and risk management in delivering services to the right recipients. According to Kostic (2024), basic identifiers such as first name, surname and date of birth can uniquely identify individuals. To enable online identification, digital identities are required. These identities are already in use across platforms such as Facebook and Google, where users create accounts with personal data and subsequently use these digital identities across multiple services. However, applying digital identity within the context of public administration introduces significantly higher sensitivity and complexity.

Early digital identity initiatives aimed to replicate personal identity in a holistic digital equivalent (Landrigan et al., 2023). Over time, several identity management models have emerged, each offering specific advantages such as scalability, privacy, or user control (Zwattendorfer et al., 2014). Landrigan et al. (2023), Podgorelec et al. (2022), and Zwattendorfer et al. (2014) compare and contrast the advantages of these models in detail.

Landrigan et al. (2023) analyze centralized, federated, and decentralized identity models. In comparison, Zwattendorfer et al. (2014) discuss isolated, central, and user-centric/decentralized models, while Podgorelec et al. (2022) include isolated, central, federated, and self-sovereign identity models. Despite minor variations, these frameworks typically share four core entities that are a Service Provider (SP), a User, an Identity Provider (IdP), and a Controlling Party (CP) responsible for enforcing regulations.

2.2.1 Isolated Model

Podgorelec et al. (2022) and Zwattendorfer et al. (2014) describe the isolated model as the simplest form of identity management. In this model, the SP and IdP are unified, meaning that authentication is performed directly by the service provider. The functions of the identity management system such as creating, maintaining, or deleting identities can only be used by the specific service provider. Therefore, the identity system is closed. Additionally, users must register individually with each service provider. Consequently, users must manage multiple credentials, which becomes burdensome and inefficient (Jøsang & Pope, 2005).

2.2.2 Central Identity Model

This model mitigates the burden of multiple registrations by storing user identity data centrally. As discussed by Landrigan et al. (2023), Podgorelec et al. (2022), and Zwattendorfer et al. (2014), the IdP handles credential issuance, authentication, and identity lifecycle management, thereby reducing duplication of identity data across SPs. Google Identity or Apple ID can be given as an example to central identity management model (Podgorelec et al., 2022).

Podgorelec et al. (2022) underline three disadvantages of the Central Identity Model. First, the central identity provider (IdP) becomes a single point of failure since the IdP stores required user identity information for all SPs. Second, the central IdP is directly involved in all authentication processes. This means that central IdP can learn which user authenticates at which service provider at what time. Lastly, in reality multiple IdPs exist, all of which serve their own set of SPs. Therefore, limited interoperability exists between IdPs and SPs, necessitating multiple registrations when trust relationships are not present.

2.2.3 Federated Model

Zwattendorfer et al. (2014) and Landrigan et al. (2023) argue that the federated model addresses these limitations by enabling trust relationships between multiple IdPs. In this "circle of trust," authentication can be delegated between entities. Rather than storing

identity data in one place, the data remains distributed but linked via a common identifier. In this model, identity data is stored in a distributed way across different identity or service providers. Thus, no single party holds complete control. European eIDAS interoperability framework, which federates national IdM systems of EU Member States to enable cross border authentication processes is a prominent example of federated IdM system (Podgorelec et al., 2022).

2.2.4 Decentralized / User-Centric Model

In all other identity management models mentioned earlier, users' data is being stored and by the IdP. Simply, users authenticate through the IdP, which then transmits the necessary identity information to service providers (Podgorelec et al., 2022). However, Podgorelec et al. (2022) argue that this centralization brings significant security and privacy concerns, as the IdP becomes a high-value target for cyberattacks. In this sense, User-centric or Decentralized Identity Model represents a shift from previously mentioned identity management systems.

Landrigan et al. (2023) emphasize that decentralized models enhance user control, reduce institutional dependency, and align with digital sovereignty goals. These systems often use blockchain or distributed ledgers to verify metadata such as public keys and credential identifiers that are necessary for verifying identity and establishing trust. The national IdM solutions relying on smartcards such as the Austrian Citizen Card or the German eID can be given as real-world implementation examples of decentralized identity model (Harbach et al., 2013; Podgorelec et al., 2022; Zwattendorfer et al., 2014).

2.2.5 Self-Sovereign Identity (SSI)

While user-centric models still depend on centralized IdPs to some extent, Self-Sovereign Identity (SSI) removes even that dependency and makes the user the sole sovereign of their credentials. Podgorelec et al. (2022) explain that enabled through peer-to-peer authentication and decentralized ledgers, users maintain complete control over their credentials. Abraham et al. (2021) support this view highlighting that credential issuance and verification achieved through central authority agnostic identity data and peer-to-peer authentication.

Podgorelec et al. (2022) give the European Self-Sovereign Identity Framework (ESSIF) as an example to SSI. Furthermore, they argue that the recent developments in identity management systems show a trend towards user-controlled identity data. In this light, the term identity wallet has attracted attention, and the trend has also been noticed by the European Commission.

2.3 eID and Cross-border Authentication in the EU

The eIDAS Regulation, introduced in 2014, marked a foundational step toward achieving cross-border digital identity interoperability within the EU. It required member states to establish national electronic identification (eID) schemes that adhere to shared technical and security standards, thereby enabling citizens to authenticate themselves across borders using their national eIDs (Zafeiropoulou & Sakkopoulos, 2023). For a long time, national eID systems were limited to national level use, which prevented authentication at foreign service providers in another Member State (Corici et al., 2022). However, cross-border authentication has become critical in a converging European society, where secure and reliable access to public-sector services across Member States is a growing expectation (Czerny et al., 2023).

Corici et al. (2022) mention that many EU member states have started to roll out their national eID systems prior to eIDAS regulation. These early implementation of national eID systems relied on smart card technologies, issuing citizens personalized smart cards to securely authenticate online service providers. Although functionally mature, these smart card–based solutions suffered from low user adoption due to usability issues. Moreover, they lacked interoperability mechanisms to support cross-border use.

Corici et al. (2022) further argue that the eIDAS framework aimed to address this gap by defining legal and technical standards, most notably through protocols like SAML2, which enabled the federation of national identity systems. However, the eIDAS regulation primarily assumed the use of web browsers on traditional end-user devices such as desktop computers or laptops. In recent years, mobile eID solutions have emerged across Member States as alternatives to smart card–based approaches. This shift raises challenges when the technical interoperability framework must operate in mobile-only environments, where smartphones replace desktops, mobile apps replace browsers, and OpenID Connect emerges as the preferred protocol due to its greater suitability for mobile environments.

Complementary EU initiatives such as the Digital Single Market (DSM) and the Single Digital Gateway Regulation (SDGR) further underscore the Union’s commitment to pan-European eGovernment services. These initiatives aim to standardize and simplify online access to public administration, regardless of a citizen's Member State (Corici et al., 2022). Together, these frameworks reflect a broader strategy to ensure that digital identity not only supports national authentication but also evolves to meet the demands of cross-border mobility and digital inclusivity within the EU.

2.4 eIDs In Estonia and Belgium

2.4.1 Estonia

According to Mander et al. (2023), the ID card has been issued in Estonia since 2002 and is the primary identification document. Approximately 99% of Estonian residents possess an ID card, which enables digital authentication and electronic signing through public key encryption (Mander et al., 2023). Since eID is not a new concept in Estonia, the country has been extensively studied in the fields of digital government and eID from various perspectives, such as digital government continuity, public-private partnership frameworks for managing eID projects, long-term identity management strategy design, and the role of the eID ecosystem as part of critical national infrastructure (Bejussova et al., 2024; Lips et al., 2019, 2023; Mander et al., 2023; Skierka, 2023).

In their work, Lips et al. (2019) examine Estonia's long-term identity management strategy, emphasizing the country's high level of e-governance maturity. Their work primarily provides insights into crisis management in the face of large-scale security risks. Similarly, Morgan and Parsovs (2017) investigate vulnerabilities in ID card chip authentication mechanisms, contributing to the development of more secure and universal solutions.

From a different angle, Bejussova et al. (2024) argue that a reliable eID is essential for advancing digitalization and establishing a stable, long-term e-governance strategy. Estonia's experience offers valuable insights given its robust track record in implementing eID solutions within a public-private ecosystem. In this context, the Estonian eID ecosystem operates as a collaborative network involving various public and private sector stakeholders, each playing a crucial role in the system's functionality.

Emphasizing public-private partnerships as a foundation for a successful eID ecosystem, both Bejussova et al. (2024) and Lips et al. (2023) map the key actors involved in Estonia's eID framework. Additionally, Bejussova et al. (2024) note that the Estonian eID ecosystem comprised of six different eID types including the mandatory ID card, Digi-ID, e-residency digital identity card, residence permit card, diplomatic identity card, and a mobile-ID solution embedded in SIM cards. Furthermore, a certified Smart-ID solution is available for authentication and signing, representing another example of public-private collaboration.

Although there is extensive literature on Estonia's eID ecosystem, academic coverage of the EUDI Wallet remains limited. To the best of the researcher's knowledge, no academic publications have yet focused on the Estonian EUDI Wallet ecosystem.

2.4.2 Belgium

A wide range of research in the academic literature focuses on Belgium's eID ecosystem and adoption, from perspectives such as eID card evolution, data privacy, multi-application usage, user access, and acceptance (De Cock et al., 2006; Dumortier & Robben, 2010; Fairchild & de Vuyst, 2012; Mariën & Van Audenhove, 2010; Somers & Dumortier, 2006). Belgium, similar to Estonia, is an early and advanced adopter of eID. De Cock et al. (2006) state that Belgium was among the first European countries to issue an eID card to all citizens aged 12 or older. Along with Estonia, Belgium maintains very high eID coverage.

De Cock et al. (2006) provide a timeline of Belgium's eID rollout, which began after the Council of Ministers approved a concept study for the eID card. The pilot phase began in March 2003, when the first four eID cards were issued to civil servants. The contract for preparing and producing the cards was awarded to the private company NV Zetes. Subsequently, the first municipality began issuing eID cards to residents on May 9, 2003, with national rollout commencing in September 2004.

In their work, Mariën and Van Audenhove (2010) provide a critical assessment of the development and deployment of Belgium's eID from societal, technical, and political perspectives. Building on this, Fairchild and de Vuyst (2012) focus on data privacy and application usage of the Belgian eID card. On the other hand, while discussing the functionalities of the eID card, Somers and Dumortier (2006) focus on the interest of both private companies and government institutions in eID applications for authentication and transactions, as well as the delayed implementation of those applications despite early interest.

While there is a substantial body of academic literature on Belgium's eID system, most of it dates back to the early stages of implementation in the mid-2000s. As with Estonia, to the best of the researcher's knowledge, there are currently no academic publications focusing specifically on the implementation of the EUDI Wallet in Belgium.

2.5 eIDAS and eIDAS 2.0 Regulations

2.5.1 eIDAS

Published in the Official Journal of the EU ten years ago, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, known as the eIDAS Regulation, established a foundational legal framework for the cross-border recognition and use of electronic identification and trust services within

the EU. Hence, the eIDAS Regulation (Regulation (EU) No 910/2014) serves as the legal foundation for secure and legally binding cross-border electronic authentication, as well as for the use of trust services, namely eSignature, eTimestamp, eID, qualified web authentication certificate, eSeal, and electronic registered delivery service in the internal market across the EU (Corici et al., 2022; Czerny et al., 2023; Van Roijen, 2024).

Lukkien et al. (2023) argue that the eIDAS Regulation introduced the first cross-border framework for trusted digital identities and trust services, facilitating secure electronic interactions between citizens, businesses, and public authorities. Its goal was to allow EU citizens to access public services across Member States using electronic identification issued in their home country, mutually recognized by all participating states.

According to Corici et al. (2022), the Regulation aims to stimulate economic activity in the EU single market by enabling companies, citizens, and public authorities to conduct secure and transparent electronic interactions. Similarly, Lukkien et al. (2023) emphasize that a key objective of eIDAS is to advance the Digital Single Market by promoting sustainable competition, protecting consumer interests, and ensuring high levels of security and trust in electronic identity solutions. To ensure interoperability of electronic identification services, eIDAS established an Interoperability Framework. This framework includes technical specifications, a set of attributes representing natural or legal persons, procedural rules, dispute resolution mechanisms, and shared security standards. Furthermore, the Regulation defines the legal effects of electronic signatures and seals, setting forth requirements for advanced and qualified versions of these instruments. In this context, eIDAS provides guidance to all relevant stakeholders such as service providers, regulators, and users on how to implement electronic transactions safely and in compliance with EU law.

Czerny et al. (2023) explain that on a technical level, cross-border authentication is enabled through a federated model, where national identity systems are interconnected. Each EU Member State operates an eIDAS Node linked to its national identity management system. These nodes form a circle of trust, allowing them to delegate authentication responsibilities across borders, as described by Landrigan et al. (2023), Podgorelec et al. (2022), and Zwattendorfer et al. (2014) under Federated Identity Management model.

2.5.2 eIDAS 2.0

Although the eIDAS Regulation (EU) No 910/2014 laid the foundational legal framework for electronic identification and trust services across the European Union, it soon became evident that the regulation required substantial revisions to align with emerging

technological needs and user expectations. As identified in the impact assessment discussed by Lukkien et al. (2023), the original regulation failed to meet the increasing demand from both public and private sectors for trusted digital identification and secure attribute exchange. Additionally, it did not address evolving user expectations for seamless and trustworthy identity solutions across borders, nor did it fully respond to rising concerns around data control and security. The regulation's scope was also found to be too limited in terms of trust services, and the lack of harmonization across Member States such as inconsistencies in supervision procedures and remote identity proofing hampered the development of a unified internal digital market.

While cross-border authentication under eIDAS has been functionally implemented across the EU, Czerny et al. (2023) note that its technical infrastructure was primarily designed for desktop-based web interactions, which were predominant at the time of the regulation’s enactment. However, the landscape has since shifted toward mobile-first usage, where smartphones and dedicated mobile applications have become the primary interface for digital services. The eIDAS framework, in its previous form, did not fully support these mobile-native scenarios, thus limiting its applicability in everyday digital interactions.

Recognizing these shortcomings, the European Commission proposed a revised regulation known as eIDAS 2.0 in June 2021, which was formally adopted in November 2022. As detailed by Lukkien et al. (2023), this proposal included a substantial amendment to Regulation 910/2014, introducing new instruments to enhance digital identity services, most notably the EUDI Wallet. The revised regulation, namely Regulation (EU) 2024/1183, was officially published in the EU’s Official Journal on April 30, 2024, as discussed by Van Roijen (2024), and marks a significant evolution in the EU’s digital identity landscape.

According to Corici et al. (2022), the primary aim of eIDAS 2.0 is to create a harmonized and secure identification service that supports new authentication methods, enabling citizens, residents, and businesses in the EU to prove their identity and authenticate themselves in all Member States using a unified digital wallet. This wallet is envisioned as a mobile application or similar digital tool that offers consistent user experience across borders, regardless of the nationality of the user.

2.6 European Digital Identity Wallet

2.6.1 Foundations and Evolution of Digital (Identity) Wallets

Even though only recently the concepts behind digital wallets have found their way to the identity management domain, the term Digital Wallet has been used in different contexts over the past few decades (Corici et al., 2022). In earlier applications, digital wallets were mostly associated with financial services. The concept of mobile wallets became particularly well established in fintech, where app-based wallets on smartphones are used to store credit card data and authorize payments at point-of-sale locations (Czerny et al., 2023).

With the evolution of user-centric identity management models, such as self-sovereign identity (SSI), digital wallets have expanded into the realm of digital identity (Corici et al., 2022; Pöhn & Hommel, 2020). Czerny et al. (2023) argue that wallet solutions such as the EUDIW rely on similar concepts and technologies as those used in financial contexts but pursue different objectives. In the identity domain, digital wallets store and transmit identity information for authentication rather than authorizing payments.

According to Corici et al. (2022) digital wallets in the identity context can be compared to physical wallets used to store and present identity cards. In the physical setting, a person presents their ID card to a third party, who then verifies their identity based on the card. In the digital setting, identity data exists in electronic form, stored in a digital wallet, and is transmitted electronically to third parties (Preukschat & Reed, 2021).

The European Digital Identity Wallet is envisioned as a secure, user-controlled tool that enables the storage and sharing of identity information in a manner comparable to how individuals present identity documents in the physical world. The primary innovation lies in decentralizing identity provision instead of national identity systems centrally managing data, the user and their wallet take on this role, thereby enhancing privacy and giving users full control over their information (Czerny et al., 2023). Czerny et al. (2023) also note that a distinguishing characteristic of the proposed wallet is its fully mobile nature.

EUDIW supports the storage of multiple digital identities within a single mobile application, giving the user exclusive control over their data. The user independently determines which data to share and with whom (Kostic, 2024). In essence, the identity wallet allows users to manage their own digital identities autonomously. Kostic (2024) identifies two central functions of an identity wallet. First, it allows for the independent storage of digital identities either by converting physical ID data into digital form or by

accepting digitally issued credentials from trusted sources. Second, it facilitates the use of these credentials by enabling users to transmit selected data to service providers. The user explicitly authorizes each data transfer and decides which data elements are disclosed (Korir et al., 2022).

2.6.2 Functional and Technical Architecture of the EUDIW

Lukkien et al. (2023) describe the EUDIW as an application that enables users to manage their personal electronic identity (eID) attributes in a trusted and secure manner through trust services. The EUDIW serves two overarching objectives. First, it supports the creation of a Digital Single Market in line with the eIDAS framework. Second, it ensures the protection of personal data as required by the GDPR.

Lukkien et al. (2023) further detail both the functional and non-functional requirements of the EUDI Wallet. Functionally, the wallet must support electronic identification, the storage and management of qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA) locally and remotely, and the ability to request and receive attestations from providers. It must also include cryptographic functions, mutual authentication with external entities, data selection and sharing capabilities, user awareness features, qualified electronic signature functionality, and interfaces for integration with external systems.

On the non-functional side, the wallet must be interoperable across the EU and conform to shared technical standards. It should provide users with full control over their data by integrating privacy and security by design. The interface must be intuitive and inclusive, supporting usability and accessibility. The wallet must enable users to share only selected data and ensure that users are informed when and how their data is being used. Furthermore, critical components must be secured in accordance with legal requirements.

2.6.3 Stakeholders

To implement the functional and non-functional requirements of the EUDI Wallet in practice, four core entities, namely the user (wallet holder), the wallet itself, the credential issuer, and the service provider, must interact (Czerny et al., 2023). Czerny et al. (2023) describe this interaction as a dynamic ecosystem, emphasizing both the credential lifecycle and the mobile-first nature of the design. The service provider offers an online service that the user wishes to access. To do so, the user must authenticate, which is achieved via the wallet transmitting identity credentials to the service provider. These credentials, however, must first be issued and stored in the wallet. This process begins with the credential issuer, who collects identity data from official sources such as national

registries authenticates it by signing it digitally and issues the credential to the user's wallet. Once in the wallet, these credentials can be used repeatedly to authenticate with various service providers.

As in other digital identity systems, this model relies on a trust framework among user or wallet holder, the wallet, the credential issuer, and the service provider. Landrigan et al. (2023) describe this framework as a set of relationships among users, identity providers, and service providers. End users must trust that service providers and identity providers will safeguard their personal information and use it only for agreed-upon purposes. Conversely, service providers rely on the identity verification performed by trusted issuers to validate user identities.

To effectively deliver identity-related services to individuals, businesses, and public institutions, the EUDI Wallet ecosystem requires multiple supporting functions. Lukkien et al. (2023) point out that these functions and roles could be provided by a single party or by specialized providers offering one or a few functions which makes the collaboration between different providers from both demand and supply side necessary. Based on the Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework (European Commission, 2023b), Lukkien et al. (2023) provides an overview of stakeholders involved in the EUDI Wallet ecosystem. These include governance bodies like national supervisory authorities, supply-side actors such as identity and trust service providers, and demand-side users including citizens, businesses, and public administrations.

Roles	Stakeholders
Governance	▪ National Accreditation Bodies ▪ National Supervisory Bodies
Supply	▪ Identity provider (eIDAS/non-eIDAS schemes) ▪ Attribute providers (eIDAS/non-eIDAS schemes) ▪ Qualified trust service provider ▪ Non-Qualified trust service provider ▪ Technology Providers ▪ Conformity Assessment body
Demand	▪ Citizens ▪ Business ▪ Public Administration
Other	▪ Public wallet service provider ▪ Private wallet service provider ▪ Public trust service provider ▪ Private trust service provider ▪ Online service providers (not-eIDAS)

Table 1: Stakeholder roles in a wallet ecosystem. Reprinted from "Barriers for Developing and Launching Digital Identity Wallets" by Lukkien et al. (2023, p. 292).

Similarly, Degen and Teubner (2024) categorize stakeholders based on the eIDAS 2.0 regulation into six ecosystem roles: issuers of identity data, wallet providers, relying

parties, users, orchestrators/regulators, and ecosystem service providers. Issuers provide identity credentials upon user request. Wallet providers supply the technical platform. Relying parties make use of identity data for business or administrative purposes. Users control their credentials. Orchestrators initiate and regulate the ecosystem, while service providers support the system's operation and compliance (Table 2).

Ecosystem Role	Description
Issuers	Issue identity data (e.g., driver's license or membership card) to the ecosystem upon the user's request
ID wallet providers	Provide a platform serving as a central wallet interface for users to store and manage their identity data
Relying parties	Utilize various identity data at the user's request to enhance shared value creation for business processes
Users	Control and manage their own identity data through a wallet application provided by the ID wallet provider
Orchestrators/regulators	Initiates the identity data ecosystem, orchestrates the value mechanisms, and oversees the regulation of activities, specific ID wallet use cases, and relying party business processes
Ecosystem service providers	Provides technical and non-technical services to support ecosystem value creation and ensure regulatory compliance for other ecosystem roles

Table 2: Ecosystem Role and Description from "Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective" by Degen and Teubner (2024, p.49)

In addition to these perspectives, Landrigan et al. (2023) consider the commercial viability of digital identity systems. For such systems to be sustainable, all participants, namely identity providers, service providers, and end users, must experience a net marginal benefit. End users benefit through enhanced service quality and convenience. Service providers may expand their reach or reduce fraud. Identity providers benefit by charging for their services. Landrigan et al. (2023) also stress the critical role of relying parties, noting that identification errors often impact them the most. Therefore, their needs and risks must be prioritized in ecosystem design.

2.6.4 Drivers and Barriers

In the literature, most of the discussion surrounding the EUDI Wallet revolves around its barriers, while only a few sources elaborate on its drivers. There is broad consensus that the main driver for the development and implementation of the wallet is the legal mandate under the revised eIDAS regulation commonly referred to as eIDAS 2.0 which establishes a harmonized framework for digital identity across the EU (Kostic, 2024).

According to Kostic (2024), this regulation not only mandates the implementation of the wallet but also highlights its potential benefits. The EUDI Wallet is expected to allow users to identify and authenticate themselves both online and offline across borders to access a wide range of public and private services. It aims to enable users to securely store, manage, and validate personal identification data and electronic attestations of attributes for the purpose of sharing them with relying parties and other users. Additionally, the wallet allows users to perform qualified electronic signatures and seals. The user-centric design ensures that individuals retain full control over their personal data and can determine what information is shared and with whom. Importantly, use of the EUDI Wallet will remain voluntary, with alternative identification and authentication methods still available.

On the other hand, a significant portion of academic literature focuses on the challenges and barriers facing EUDI Wallet implementation. Lukkien et al. (2023) offer a comprehensive categorization of empirical barriers encountered by policymakers and wallet providers. Drawing on the public service innovation literature, they identify four major categories that are organizational barriers, interaction-specific barriers between innovation partners, barriers related to perceived characteristics of innovation, and contextual barriers.

Based on their expert workshop conducted in the Netherlands, they identified several key findings. First, citizens require greater confidence in the wallet and its use. Second, while monopolies may increase user costs, they could also reduce coordination and transaction costs if appropriately regulated citing examples such as Dutch Railways and itsme in Belgium. Third, the current business case for the wallet is misaligned, although this could be improved through appropriate pricing models. Fourth, a lack of trust is compounded by the number and unfamiliarity of actors involved in the ecosystem. Fifth, a clear consensus emerged regarding the lack of standardization across systems. Sixth, concerns were raised that a government-issued wallet might hinder market development unless it plays by the same rules as private competitors to maintain a level playing field. Seventh, uncertainty about legal frameworks causes delays; although careful legislation is welcomed, some argued that collaboration could begin under a system of agreements without waiting for new laws. Eighth, there is a lack of boundary resources defined as shared standards, tools, procedures, and governance structures needed for cooperation between stakeholders. Questions remain over whether public or private actors should lead their development. Ninth, government roles are too intertwined, as they simultaneously act as policymakers, service providers, data providers, potential wallet providers, and regulators.

Kostic (2024) contributes to this discussion by emphasizing usability issues. Existing wallet prototypes suffered from poor usability, prompting the development of a low-fidelity prototype in 2020. This version aimed not only to visualize the wallet's features such as storing a national ID or driver's license but also to test usability and comprehensibility in user studies. Research indicates that users were not adequately informed about the wallet's benefits, leading to resistance in adoption. Khayretdinova et al. (2022) conducted a usability study involving 18 users of SSI-based Identity Wallets. They found that users did not perceive tangible privacy or security benefits and were confused by poorly explained terminology. These issues contributed to user reluctance to share personal data. Additionally, users prioritized usability over privacy and security, further highlighting how poor user experience can undermine trust.

Lastly Degen and Teubner (2024) argue that for eIDAS 2.0 to succeed in establishing a sustainable public–private ecosystem, robust public operating models and viable business cases are necessary to attract private sector participation. However, government-provided data often falls short of expectations, creating barriers for non-government actors and inhibiting co-creation and innovation. Furthermore, system design, regulatory conditions, and organizational structure significantly affect success. Potential collaboration between public entities and private sector actors especially banks depend on well-defined governance models for public–private partnerships. Technical and political developments are deeply intertwined and mutually influential in this process.

2.6.5 The European Digital Identity Wallet: Use Cases

Even though the literature on the EUDI Wallet is still emerging, several academic studies have begun exploring its potential applications across different sectors. Van Roijen (2024) highlights several use cases in the healthcare sector, emphasizing the wallet's role in improving data access, interoperability, and user control.

First, the EUDI Wallet could serve as a trusted and secure platform for individuals to collect and access their personal health data. This data may include both clinical information collected through interactions with public or private health services and person-generated data, such as self-reported metrics or sensor-based measurements from wearables.

Second, the wallet is designed to empower citizens with greater control over their data including health information, enabling them to actively share data with various stakeholders involved in their care whether direct, indirect, or informal. Users can also manage the granularity of the data they choose to share, maintaining autonomy over sensitive information when interacting with third parties.

The third benefit of the EUDI Wallet is its potential to facilitate cross-border healthcare services. Van Roijen (2024) suggests that the wallet could simplify scenarios involving treatment in foreign EU countries or sharing medical records across borders.

Lastly, despite the growing availability of digital health tools, their adoption has been hindered by issues like poor interoperability, fragmented data silos, repetitive input requirements, and data security concerns. EUDI Wallet could address these issues by adhering to the "once-only" principle, enabling secure and streamlined data access. In doing so, the wallet could build trust and encourage the integration of digital technologies into everyday clinical routines.

From a different perspective, Fridell et al. (2023) explore how the EUDI Wallet could be applied in the education sector. Their research focuses on EMREX, a solution designed to enable the international transfer of student data in a machine-readable format. Originating from an EU-funded project (2015–2017), EMREX aims to improve the credit transfer process following student exchanges.

In this context, EMREX requires unique identification of users in multiple countries. While the original eIDAS regulation was considered as a solution, it ultimately fell short due to usability and implementation limitations. In contrast, the EUDI Wallet offers a more user-centric and adaptable approach, aligning well with EMREX's operational model.

The flexibility of the wallet allows various applications to connect and utilize the stored data independently, making it an attractive solution. As a result, some EMREX partners joined the Digital Credentials for Europe project, involving 80 organizations across 23 countries, with the goal of developing a pilot wallet installation compatible with the EUDI framework. This wallet would be able to transport educational data in the ELMO format at the user's request, demonstrating the practical feasibility of EUDI Wallet use in academic mobility.

3 Theoretical Framework and The Common Terminology

As previously stated, the overarching goal of this study is to examine the factors shaping the implementation strategies of the European Digital Identity Wallet in Estonia and Belgium, with the broader aim of deriving insights that can inform other EU Member States in their own deployment efforts. Given the multifaceted nature of digital identity ecosystems and the cross-sectoral collaboration they require, this study seeks to provide a structured understanding of the key actors involved, their roles, interests, and objectives.

To this end, the research builds on a theoretical framework that is structured around two central perspectives, namely Actor-Network Theory (ANT) and PESTEL. ANT is applied to identify and analyze the complex configurations of human and non-human actors involved in the implementation of the EUDIW, while PESTEL enables a structured exploration of the external drivers and barriers impacting the digital identity wallet ecosystems and national strategies. Before introducing these frameworks, however, it is necessary to define the core concepts that form the terminological foundation of the study. This section clarifies the key terms European Digital Identity Wallet, stakeholders, as well as drivers and barriers to establish a shared conceptual basis and reduce interpretive ambiguity.

3.1 Establishing a Common Terminology

3.1.1 The European Digital Identity Wallet

Throughout this research, the terms “European Digital Identity Wallet,” “EU Digital Identity Wallet,” and “EUDI Wallet” will be used interchangeably. This interchangeable usage reflects prevailing conventions in both academic and grey literature, although the primary term used in this study will be “European Digital Identity Wallet (EUDIW),” as it corresponds with the terminology used in official EU documentation.

Beyond its various names, the term European Digital Identity Wallet is itself multifaceted, as it encompasses multiple concepts, including identity, digitalization, and the wallet. Moreover, its significance can be further extended by emphasizing the implicit connection between the digital identity wallet and data. The term wallet does not simply refer to a software application but encapsulates the broader EU ambition of providing every European citizen with a secure, standardized, and interoperable means of managing digital identity credentials. According to the EU Architecture Reference Framework (2023b), the EUDIW refers to the complete product and service offering managed by an EUDI Wallet Provider and made available to all users of that solution. The wallet is thus both a technical system and a regulatory construct, enabling individuals to access public

and private sector services, store and present credentials, and conduct trusted digital interactions. The system is closely tied to trust services under eIDAS 2.0, including electronic signatures, seals, and attestations of attributes.

The definitional complexity of EUDIW reflects its socio-technical nature. It is not only a tool for personal data management but also a mechanism through which new forms of digital citizenship, data sovereignty, and cross-border interoperability are articulated. For this reason, the EUDIW is best understood not as a static product but as an evolving digital infrastructure, shaped by a constellation of legal mandates, technical standards, institutional actors, and user practices.

3.1.2 Stakeholders

The definition of stakeholder is contextual. According to Miles (2017), stakeholder is an essentially contested concept and does not have a universal definition. Therefore, it is important to consider jointly the impact of power, interest and influence so that a distinction can be made between active influence (influencer), passive influence (collaborator), the potential to influence (claimants) and no influence (recipients). In the context of digital identity ecosystems, this study adopts an actor-relational perspective informed by Actor-Network Theory (ANT). Accordingly, stakeholders are defined not solely by their institutional status or formal role, but by their capacity to affect or be affected by the EUDIW as a socio-technical system.

Integrating insights from Pouloudi et al. (2004), this study recognizes that stakeholder roles are dynamic, overlapping, and evolving over time. Some actors possess the power to directly shape design and implementation decisions such as ministries, regulatory agencies, while others, such as end users or civil society groups, may exert influence through public discourse, adoption behavior, or resistance.

This perspective is especially relevant in the EUDIW context, where the boundary between implementers and beneficiaries is often blurred. The framework also acknowledges the agency of non-human stakeholders, such as technical artefacts, standards, and infrastructures, whose behavior and design significantly influence the system’s trajectory. This extension beyond human actors is crucial to capturing the full complexity of the EUDIW ecosystem.

3.1.3 Drivers and Barriers

For the purposes of this study, drivers are defined as factors that facilitate, motivate, or accelerate the implementation of the EUDIW, while barriers are those that inhibit, obstruct, or delay the process. These may stem from institutional, political, economic,

social, technological, or legal sources. Importantly, drivers and barriers are not always objectively identifiable. They are often constructed through stakeholder interpretations, shaped by varying interests, risk assessments, and contextual factors.

To ensure conceptual clarity and analytical consistency, this study categorizes drivers and barriers using the PESTEL (Political, Economic, Social, Technological, Environmental, and Legal) framework. This approach not only aligns with the second sub-research question but also provides a structured lens through which external influences can be systematically analyzed.

3.2 Theoretical Framework

3.2.1 Actor-Network Theory (ANT)

Actor-Network Theory (ANT) serves as one of the two main theoretical frameworks of this research. Originally formulated by Callon (1984), Latour (1996), and Law (1992), ANT offers a distinctive lens for understanding sociotechnical systems by rejecting traditional separations between the social and the technical. Rather than viewing technology as a neutral tool shaped solely by human intention, ANT posits that both human and non-human entities ranging from institutions and individuals to algorithms, standards, and digital platforms act as actors within a network that co-produces outcomes.

According to Elbanna, (2012), the foundational idea behind ANT is that in order for an actor to pursue and realize a particular goal, it must build a network of stable alliances. This is particularly relevant in the context of EUDIW, where public institutions, technology providers, regulatory bodies, and digital infrastructures must cooperate across national and supranational boundaries to enable secure, interoperable digital identity solutions. By conceptualizing the EUDIW as a dynamic socio-technical network, ANT allows this study to examine not just stakeholder identities but the processes through which they are enrolled, aligned, and sometimes contested.

Network building, performance of power and global/local relationship are the three key ANT propositions. First, the network building is realized through translation. In comparison to linear models of stakeholder interaction, ANT emphasizes the importance of translation a process by which a focal actor recruits and aligns other entities into a coherent network. Elbanna (2012) draws on Callon’s (1986) four interrelated phases of translation to explain how networks are formed, namely problematization, interessement, enrollment, and mobilization. Problematization involves framing a specific pathway as obligatory for others, effectively positioning the actor's vision as indispensable. Interessement describes efforts to break or weaken existing ties between actors and

alternative networks in order to draw them into a new configuration. Enrollment refers to the negotiation of roles and responsibilities, while mobilization involves stabilizing the network by ensuring that key actors represent and speak for broader constituencies.

This framework is particularly useful for understanding how specific national actors in Estonia and Belgium position their EUDIW strategies as central to EU digital identity goals, thereby attempting to enroll both domestic and European stakeholders in their model. For instance, a national digital identity agency may seek to act as an obligatory passage point by aligning its own implementation logic with EU-wide standards such as eIDAS 2.0. Thus, persuading other actors such as private sector developers or municipal authorities to work through its systems.

ANT's second core proposition concerns the nature of power. Rather than conceptualizing power as something that actors possess and exert, ANT views power as an effect of network stability. As Elbanna (2012) argues, artefacts such as identity verification tools, wallet interfaces, or digital signature algorithms are not passive instruments; they participate actively in shaping the network's behavior. In this view, power is performed through durable actor alignments and the consistent reproduction of a shared order. This relational view of power is especially relevant in the EUDIW context, where authority does not flow top-down but emerges from the alignment of legal mandates, technical standards, and stakeholder participation.

The third key dimension of ANT is its rejection of fixed scales such as global versus local or macro versus micro. Instead, ANT adopts a flat ontology, treating all actors symmetrically and emphasizing how global effects such as EU-wide interoperability emerge from local translations and stabilizations. As Elbanna (2012) notes, the distinction between global and local is itself a result of strategic network-building. In the EUDIW case, this perspective allows the research to move beyond national comparisons in isolation and instead trace how local practices in Estonia and Belgium participate in constructing European digital identity infrastructures.

Critically, however, ANT is not without its limitations. It has been criticized for flattening all actors to the same analytical level, potentially underemphasizing structural inequalities, institutional inertia, or historically embedded forms of power (Whittle & Spicer, 2008). In the context of EUDIW, this raises important questions about how to reconcile ANT's relational dynamics with persistent asymmetries in digital capacity or political influence within or among Member States. To address this concern, the present research uses ANT not in isolation but in conjunction with PESTEL, which provides a complementary macro-level lens to capture structural drivers and barriers.

In this research, Actor-Network Theory serves three purposes. First, it frames the European Digital Identity Wallet not merely as a technological artifact, but as a dynamic network involving a wide range of human and non-human actors engaged in ongoing translation processes. Second, it provides a structured approach for interview design, data collection, analysis, and stakeholder mapping, highlighting their relationships and interactions. Third, ANT provides the analytical foundation for answering the first sub-research question, which focuses on identifying and mapping the key stakeholders involved in EUDIW implementation in Estonia and Belgium.

In this context, to provide an extensive answer for the first sub-research question, this study draws on Pouloudi et al.'s (2004) framework for stakeholder identification in information systems. Building on Freeman's (1984) definition of organizational stakeholders for information systems which is "A stakeholder of an information system is any individual, group, organization or institution who can affect or be affected by the information system under study" (p.706), Pouloudi et al. (2004) develop a dynamic, iterative model that aligns closely with the relational and performative logic of ANT.

Pouloudi et al.'s (2004) emphasizes seven guiding principles for identifying stakeholders. These include the importance of timing and context, the interdependence of stakeholders, the evolving nature of roles, the potential for multiple simultaneous roles, and the variability of stakeholder interests over time. Importantly, the final principle acknowledges that some stakeholders may lack the capacity to act upon or advance their interests, revealing latent power imbalances even within symmetrical networks. This last point is especially salient in the EUDIW case, where marginalized user groups or smaller Member States may have limited influence over standard-setting processes, despite being theoretically included in the network.

Principles of Stakeholder Behavior	**Implications for Stakeholder Identification and Analysis**
1) The set and number of stakeholders are context and time dependent	• Stakeholder map should reflect the context • Stakeholder map should be reviewed over time
2) Stakeholders cannot be viewed in isolation	• Consider how stakeholders are linked
3) A stakeholder's role may change over time	• Adopt a long-term perspective
4) Stakeholders may have multiple roles	• Study how perceptions change

5) Different stakeholders may have different perspectives and wishes	• There are different versions of the stakeholder map to be drawn
6) The viewpoints and wishes of stakeholders may change over time	• These different versions of the stakeholder map should be reviewed over time
7) Stakeholders may be unable to serve their interests or realize their wishes	• Need to consider political issues (as well as technical, economic or other)

Table 3: How Stakeholder Analysis Can Be Mobilized With Actor-network Theory To Identify Actors by Pouloudi et al. (2004, p.707)

Thus, the ANT framework augmented by Pouloudi et al.'s (2004) operational model provides both a conceptual and practical foundation for identifying and analyzing stakeholder dynamics in EUDIW implementation. By combining a granular, actor-focused perspective with iterative stakeholder mapping, it offers a powerful tool for examining how technical, institutional, and political alignments emerge and how they may be contested within the evolving European digital identity wallet landscape.

3.2.2 PESTEL

As previously discussed, while stakeholder dynamics and network interactions play a crucial role in shaping the implementation of the European Digital Identity Wallet, these dynamics are not formed in a vacuum. They are shaped, constrained, and enabled by a range of external structural factors. To capture these influences systematically, this research adopts the PESTEL (Political, Economic, Social, Technological, Environmental, and Legal) framework as its second major analytical lens. Whereas Actor-Network Theory illuminates the micro-level negotiations and alignments between actors, PESTEL allows the study to address the broader macro-environmental conditions that act as drivers or barriers to EUDIW implementation in Estonia and Belgium.

Originally developed in strategic management and policy planning, PESTEL is designed to identify and assess the external conditions influencing organizational or systemic change (Cadle et al., 2010). Although often applied to market environments, its flexibility has enabled scholars to use it in diverse contexts from cybersecurity education (Ricci et al., 2021) to political hacktivism (Nurmi & Niemelä, 2018). This versatility makes it a suitable tool for digital governance research, especially in assessing how national and supranational factors interact to influence technology adoption.

In this research, PESTEL is used not to describe a passive environment, but as a conceptual lens to critically investigate how macro-level forces shape actor behavior, strategic choices, and system design in the context of EUDIW adoption. This is

particularly important given the heterogeneity across Member States in terms of digital infrastructure, administrative traditions, regulatory cultures, and public trust in digital governance. A shared European framework such as EUDIW cannot succeed unless these macro-level differences are understood, navigated, and, where possible, harmonized.

The PESTEL framework in this study is governed by two guiding principles, adapted from Cadle et al. (2010), first, it focuses only on factors that are external to the direct control of the actors under study. Second, it considers only those factors that significantly influence the implementation of the EUDIW. These criteria are essential for distinguishing between manageable organizational choices and broader structural constraints or enablers.

Each domain of the PESTEL framework is understood in the following terms within this study. Political factors include national government priorities, intergovernmental coordination, the role of EU institutions, and political support or resistance to digital identity systems. Economic factors concern the availability of funding, cost structures for development and maintenance, market incentives for private sector actors, and the economic rationales underpinning interoperability initiatives. Social factors refer to public trust, digital literacy, cultural attitudes toward privacy and surveillance, and levels of citizen engagement with digital services. Technological factors address the maturity of national digital ecosystems, interoperability frameworks, data security standards, and the presence of legacy systems. Environmental factors might include energy consumption of digital infrastructure or sustainability targets related to digital transformation. Legal factors involve the regulatory landscape at both the EU and national levels, including GDPR compliance, eIDAS 2.0 mandates, data protection regimes, and certification schemes.

Unlike more descriptive uses of PESTEL, this research applies the framework interpretively and comparatively. That is, it is used not only to categorize external conditions, but also to analyze how these conditions are perceived and acted upon differently by stakeholders in Estonia and Belgium. The comparative approach highlights not just what barriers or drivers exist, but how different political and institutional contexts mediate their effects.

Furthermore, the PESTEL framework does not operate in isolation within this study. It is methodologically integrated with Actor-Network Theory to enrich the analysis of stakeholder dynamics. For example, while ANT identifies a national wallet provider as a key actor, PESTEL explains why that authority is constrained by funding shortages (economic factor), shaped by data protection regulation (legal factor), or compelled to act within a broader EU mandate (political factor).

Finally, PESTEL also informs the research design and data collection strategy. Interview guide was developed to elicit perceptions of external constraints and enablers across the six domains of the framework. This structured yet open-ended approach ensures that both theory-driven and emergent insights can be captured (Fereday & Muir-Cochrane, 2006). Additionally, where possible, documentary analysis is used to triangulate interview data, adding depth and contextual richness to the PESTEL assessment (Bowen, 2009).

In summary, the PESTEL framework plays three interrelated roles in this research. First, it structures the analysis of macro-level factors shaping the EUDIW implementation process. Second, it complements Actor-Network Theory by contextualizing stakeholder behavior within broader systemic conditions. Third, it directly supports the analysis of the second sub-research question, which focuses on the drivers and barriers affecting stakeholder engagement in the EUDIW implementation in Estonia and Belgium.

4 Methodology

To showcase the validity and reliability of findings as well to ensure their generalizability, this chapter outlines the methodology which this research was built on. In the research, a qualitative multi-method based on document analysis and semi-structured expert interviews has been applied focusing on the cases of Estonia and Belgium in European Digital identity Wallet implementation. Despite the use of both methods, while semi-structured expert interviews were the main data collection method, document analysis was used to complement as well as cross-check insights between the expert interviews and the document data. By doing so, to analyze the data collected from these sources, combination of inductive and deductive approaches was followed.

A qualitative multiple-case study has been chosen to study Estonian and Belgian cases in European Digital Identity Wallet to draw insights that can inform a broader EU rollout, offering a reference for other cases of EUDIW implementation. Compared to single-case studies, multiple-case studies add observations for study without taking the research design into more quantitative ground (Stewart, 2012). Stewart (2012) argues that in multi-case studies, various instances of a particular phenomenon are brought together in order to identify as well as investigate key factors that seem to have an impact on an outcome. Furthermore, stemming from this, multi-case research enables the researchers to use inductive and deductive methods to investigate the relative effectiveness of specific approaches. Therefore, because of its strength coming from its capacity to feature variance on the dependent variable and because it fits with the research methods mentioned above, multiple-case study approach has been chosen for this research.

In addition to building on the existing academic literature, the data utilized to study the cases of Estonia and Belgium originate from semi-structured expert interviews as well as official documents including regulations published by the EU institutions, European Digital Identity Wallet toolbox documents and implementing acts. Since the research utilizes qualitative multi-method combining document analysis and semi-structured expert interviews, to enhance the robustness and credibility of the results, and to provide a comprehensive answer to the research questions, methodological triangulation is applied in line with the guidelines of Jack and Raturi (2006). This approach involves developing a well-structured triangulation strategy, employing methods that mitigate each other's limitations, and ensuring that the findings are generalizable.

Methodological triangulation strengthens the validity of a research conclusion more than any single method alone. Morgan (2022) argues that triangulation is a strategy designed to increase the trustworthiness of research by using different methods to gather information. In this way, findings can be confirmed across data sets, which minimizes the

possibilities for biases. Hence, triangulation helps to determine if the findings of a study are consistent and to develop a deeper understanding of the topic being investigated. In this study, the combination of document analysis and expert interviews ensures completeness by addressing the inherent limitations of each method while enhancing the depth and reliability of the findings.

To analyze the data gathered, inductive as well as deductive elements, in other words, an inductive-deductive hybrid analysis has been performed. In this context, Fereday and Muir-Cochrane's (2006) work on interpreting raw data in a doctoral study on the role of performance feedback in the self-assessment of nursing practice by using a hybrid process of inductive and deductive thematic analysis has been utilized for guidance and their inductive-deductive hybrid analysis technique has been adapted to the context of this research. Hence, following Fereday and Muir-Cochrane's (2006) model, the analysis in this research began with a preliminary coding scheme informed by theory and EU-level documents, which was then revised and expanded through the identification of new, emergent themes in the empirical data coming from the interviews as well as national documents.

The deductive or top-down approach ensures that pre-defined theories and/or concepts are being taken into account. On the other hand, the bottom-up, inductive approach creates room for new themes and/or concepts not mentioned in literature. Additionally, it allows alternative interpretations of a particular topic, reducing bias if the pre-existing theory is flawed or incomplete. In this context, in order to answer the research questions of this study, more specifically, to identify stakeholders and their roles, explore drivers and barriers, compare implementation strategies of EUDIW in Estonia and Belgium a preliminary coding scheme for thematic analysis has been created based on the Actor Network Theory, PESTEL frameworks, official EU documents as well as academic literature. Afterwards, the bottom-up, inductive approach has been followed on the one hand to generate additional themes from the expert interviews and official documents published by the Estonian and Belgian governments, to capture country-specific nuances to answer research questions on the other hand.

In addition to the software solutions detailed in the subsequent sections of this chapter, two AI-based tools were used to support the research process. The first is ChatGPT, a natural language processing tool based on the GPT-4 architecture. It was employed exclusively to improve the quality of writing by enhancing clarity, coherence, and readability of selected text segments. At no point was it used for generating original research content or analysis. The second tool is the online platform Kumu.io, which was utilized to map the European Digital Identity Wallet ecosystems in Belgium and Estonia.

This visual mapping helped to conceptualize the complex networks of actors and relationships involved in each national context.

In light of this information, the following subchapters elaborate the methodologies performed in this study. In line with their implementation order, literature review, document analysis, and expert interviews are introduced. At the end, the chapter concludes with the limitations stemming from the chosen methodologies.

4.1 Literature Review

By combining findings and perspectives from various empirical studies, a well-conducted and effective literature review creates a solid foundation for a firm data collection and analysis (Snyder, 2019). In this research, a literature review was systematically carried out prior to document analysis and expert interviews to inform the deductive phase of the thematic analysis. In other words, the literature review was used to gather initial insights into each research question. Specifically, it helped with identifying key stakeholders and their roles in the EUDIW implementation, potential drivers and barriers, and existing implementation strategies across the EU. These insights guided the development of a preliminary coding framework used during data analysis. This ensured that the research was firmly grounded in the existing academic literature and contributed to the digital identity field by filling a gap through a case study on Estonia and Belgium.

A literature review method inspired by Systematic Literature Review (SLR) is conducted to map the available literature in the EUDIW context following the guidelines of Kitchenham et al. (2010). In light of these guidelines, a three-step process consisting of database selection, literature search, and literature selection has been followed. Finally, as discussed earlier, in line with the ANT and PESTEL theoretical frameworks, as a deductive top-down approach, the concepts found in the selected articles particularly those related to stakeholder roles, implementation drivers/barriers, and strategies have been incorporated into the coding scheme to be used in the data analysis for the expert interviews as well as document analysis.

Following the process guidelines of Kitchenham et al. (2010), the Web of Science, Scopus, and Limo databases were selected for their comprehensive, curated, multi-disciplinary coverage of scholarly literature. To systematically identify relevant studies related to the European Digital Identity Wallet, search queries were constructed using combinations of key terms such as “digital identity wallet”, “eIDAS 2.0”, “digital identity”, “eID”, and “European Digital Identity Wallet”. AND/OR Boolean operators were used while creating search queries. AND operator was used to combine distinct

concepts, while the OR operator was used to group synonyms such as “digital identity” OR “eID”.

An iterative search process was employed to ensure comprehensive coverage of the topic. As the research progressed, the literature review was continuously expanded and refined until thematic saturation was reached, adequately capturing the key concepts relevant to the scope of this study. Studies not written in English or without full-text availability were excluded. Furthermore, due to the contemporariness of the topic as well as limited number of academic articles, only eleven directly relevant articles on the European Digital Identity Wallet were identified. To address this scarcity, backward and forward snowballing (Wohlin et al., 2022) was employed based on existing studies. This way additional literature from adjacent fields to digital identity wallet including information systems, public administration, eGovernment, eGovernance, and digital policy was identified.

4.2 Document Analysis

Document analysis is a systematic procedure for reviewing and evaluating various documents including books, newspaper articles, academic journal articles, and institutional reports in order to find, select, make sense of and synthesize data. Morgan (2022) argues that even though the data pre-exists in the documents without any data creation actions by the researcher, the documents reflect the beliefs of people in a similar way to the data a researcher would collect from interviews. Thus, researchers must be active in discovering, collecting, and interpreting insights from the data in order to elicit meaning as well as making decisions regarding which materials will be analyzed and which ones will be excluded to develop empirical knowledge (Bowen, 2009).

Document analysis has often been used together with other research methods as a means of triangulation to supplement and corroborate findings across different data sets, to increase the trustworthiness of a study, to reduce the impact of the potential biases, and to ensure the consistency of the findings in a study (Mackieson et al., 2019; H. Morgan, 2022). In this context, document analysis as a complementary data collection procedure in support of expert interviews has been selected for this study due to three reasons. First, document analysis played a role in ensuring the impartiality of the data combined with as well as by supplementing expert interviews. Data collected from the documents and expert interviews cross-checked and incorporated with one another. Second, in line with the first reason, combined with interviews, document analysis has provided a more complete understanding of the EUDIW implementation across the EU by providing the implementation roadmap for the countries. In other words, the document analysis has provided a basis for the EUDIW implementation and regulations that country cases of

Estonia and Belgium have built on. Therefore, supplemented by the expert interviews, document analysis has provided an overview of the EUDIW implementation roadmap in Estonia and Belgium. Lastly, as discussed in previous sections, academic research on the European Digital Identity Wallet is still in its early stages, with a primary focus on technical aspects such as security and privacy (Lukkien et al., 2023). On the other hand, there are official documents published by the EU Institutions and regulatory bodies consisting of essential information regarding EUDIW implementation requirements, regulations, guidance and ecosystem actors.

Following these three reasons, in this research, document analysis has served two purposes. First, following the literature review, analysis of the EU level documents contributed to the deductive phase of the thematic analysis. It has been used to gather insights for research questions. Particularly, the method was applied to gather data for identifying key stakeholders and their roles, potential drivers and barriers, and implementation guidelines as mentioned earlier. These insights, combined with the ones acquired from literature guided the development of a preliminary coding framework used during the data analysis. Second, combined with the insights collected from the literature, information gathered from the documents used to tailor the interview questions aiming to address the information gaps in the documents as well as the literature especially in the specific country cases of Estonia and Belgium in terms of which roles defined by the implementing acts have been embarked on by which actors, which stakeholders are involved in the Estonian and Belgian ecosystems, what are the drivers and barriers for these stakeholders, to capture the specific stakeholder perspectives and in order to address the research questions.

4.2.1 Document Selection

In light of Morgan's (2022) guidelines, a three-step process consisting of document selection, sampling, and thematic analysis of the documents has been followed. In the document selection phase, firstly, the documents that are not written in English, that are not primary source or published by the EU institutions or regulatory bodies have been excluded. Therefore, most of the national level documents from Estonia and Belgium had to be excluded due to their availability only in Estonian, French, Dutch, and German. Since the European Digital Identity Wallet is a new topic, and the published documents are recent and up to date, publication dates have not been considered as a selection or exclusion criteria. After this step, to further curate the document selection, four factors namely authenticity, credibility, representativeness, and meaning principles have been considered as highlighted by Morgan (2022). According to Morgan (2022), first, authenticity means the extent to which a document is genuine. In other words, the

document is free from containing inconsistent content, errors, not coming from an unreliable secondary source and it is not modified to reflect a particular perspective. The credibility principle highlights the extent to which the source is free from error and distortion. Third, representativeness focuses on how typical a document is and its freeness from idiosyncratic content. Lastly, meaning puts emphasis on a document's content as well as whether the evidence is clear and understandable.

Hence, authenticity, credibility, representativeness, and meaning are foundational elements to ensure the objectivity and trustworthiness of research. In order to ensure compatibility with these principles, to ensure that the documents were credible, representative of the European Digital Identity Wallet in both Estonian and Belgian cases, as well as the documents' literal and interpretive meanings connected to the European Digital Identity Wallet context, this study extracted documents only from the EU Institutions official websites such as the European Commission, European Parliament as well as the Official Journal of the European Union.

4.2.2 Sampling

As the second step of document analysis based on Morgan's (2022) guidelines, purposive sampling method has been followed to construct the collection of documents that allowed this research to answer the research questions together with expert interviews. In this sense, purposive sampling has been utilized to select EU level documents that are most likely to yield appropriate and useful information as well as to identify and select documents that uses limited research resources effectively.

The number of documents needed to collect and draw meaningful data was not determined prior to the research. As was the case in the literature review, an iterative search process was employed to ensure comprehensive coverage of the topic. As the research progressed, the document analysis was continuously expanded and refined until thematic saturation was reached, adequately capturing the key concepts relevant to the scope of this study.

Google has been selected as the search engine to navigate and determine the initial documents published by the EU institutions and the search has been launched with the key term "European Digital Identity Wallet". Using a snowball searching approach by taking Wohlin et al.'s (2022) work as an example, the document search progressed by navigating from one webpage to another through embedded hyperlinks, progressively expanding the exploration of the topic, starting from the European Commission's European Digital Identity Wallet webpage.

As a result of the sampling process, four documents totaling 198 pages have been identified in .pdf format. Then uploaded to MAXQDA, a software for qualitative data analysis for the coding and thematic analysis.

Documents Selected	Data Analyzed
European Digital Identity Impact Assessment Report (2021)	• EUDI Wallet Barriers
The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework (2023)	• Roles in the EUDI Wallet Ecosystem • Definitions of terms relevant to the Architecture and Reference Framework
European Digital Identity Regulation (2024)	• EUDI Wallet Drivers
Implementing Regulation: Rules for the Integrity and Core Functionalities of eID Wallets	• Requirements for EUDI Wallet • EUDI Wallet Drivers and Barriers

Table 4: List of documents

4.2.3 Thematic Analysis of the Documents

After the documents were selected, the analysis proceeded to the third step, namely the thematic analysis of the documents. Thematic analysis was selected since it enables researchers to identify and interpret as well as extract patterns of meaning in the data (Mackieson et al., 2019). Similarly, Clarke and Braun (2017) describe thematic analysis as a method to identify, analyze and interpret patterns of meaning, or themes, within qualitative data, which can be applied across a range of theoretical perspectives.

In this research thematic analysis was used for both document and expert interview data to identify and interpret recurring patterns, so called themes. Inspired by Mackieson et al. (2019), a three-level analytical process was followed. In the first level, preliminary codes and themes were identified based on relevant academic literature and this study's chosen theoretical frameworks. In the second level, codes were refined, adjusted, and confirmed for consistency. In the third level, these codes were used to cross-check insights between the expert interviews and the document data, and vice versa.

Following Bowen's (2009) approach to triangulation between document analysis and expert interviews, an initial set of codes was generated based on the theoretical frameworks and relevant literature after transcribing the interviews. To ensure effective triangulation, both data sets were analyzed together, allowing themes to emerge across the entire corpus. Since the document analysis was intended to complement the interviews, a semantic thematic analysis was applied to the documents to examine their explicit content. Then, these findings were fed into the interview analysis, where a latent, in other words, interpretive thematic analysis was applied to explore underlying meanings, discourses, and assumptions.

Theoretical, so called deductive, thematic analysis approach was taken, in which codes and themes were guided by the research's theoretical frameworks, Actor Network Theory (ANT) and PESTEL. This allowed the analysis to be anchored in established analytical categories, such as actor roles, technological, political, and socio-economic influences. Thus, coding was initially organized according to the main research question and its three sub-questions, forming the backbone of the coding scheme.

Following this initial stage, the identified codes were grouped into tentative themes that reflected the evolving data. As the research progressed, connections among codes and themes were continuously reviewed and refined. The coded data were regularly evaluated in relation to the complete data set to ensure internal coherence. Codes that proved irrelevant or redundant were excluded, while overlooked patterns were incorporated. This iterative process continued until further refinements did not affect the research outcomes. In other words, when the thematic saturation was reached.

Subsequently, the finalized themes and sub-themes were clearly named and defined in alignment with the research questions. The final thematic structure derived from the document analysis consisted of four main themes and twelve sub-themes. The first main theme, Institutional Roles and Ecosystem Definitions, centers on how responsibilities and roles are distributed within the EUDIW landscape. Within this theme, three sub-themes were identified namely, "Government Agency Role", "Private Sector Participation", and "EUDI Ecosystem Definitions". The second main theme, Regulatory and Technical Foundations, reflects the core legal and architectural structures underpinning the implementation of the EUDIW. It includes three sub-themes namely, "Legal Artefacts as Non-Human Actors", "Certification Requirements", and "Architecture and Reference Framework (ARF)". The third main theme, Political and Legal Drivers, emphasizes the macro-level rationales and legal mandates driving EUDIW adoption at the national level. Within this theme, three sub-themes emerged, which are Strategic Autonomy and Data Sovereignty", "Mandated Public Provisioning", and "European Integration Goals". The fourth and final main theme, Barriers to Interoperability and Implementation, captures the structural, technical, and institutional challenges encountered during the rollout of the EUDIW that are "Device-Level Security Risks", "Unstable Legal Foundations", and "Lack of Reference Implementation".

Overall, the thematic analysis followed a hybrid approach, combining deductive, so called theory-driven and inductive namely, data-driven coding, particularly in the document stage. Thematic refinement continued in the analysis of expert interviews, allowing for deeper insight and cross-validation between institutional and expert perspectives. The

inductive coding approach of the thematic analysis process is elaborated further in the section on the thematic analysis of the expert interviews.

4.3 Expert Interviews

Following the literature review and the document analysis, semi-structured expert interviews were conducted which served two functions in this research. First, the insights gained from expert interviews were utilized to explore and answer the research questions of this study. Particularly, expert interviews have been used to gather data on the key stakeholders in Estonia and Belgium involved in the adoption and implementation of the EUDIW, and their roles, interests, and objectives as well as the drivers and barriers for the stakeholders in EUDIW implementation and lessons that can be drawn for the broader EU rollout of the wallet. In other words, expert interviews were the main source of data in this research to answer the main as well as the three sub-research questions but complemented by the document analysis with triangulation to enhance the robustness and credibility of the results, and to provide a comprehensive answer to the research questions. Second, to cross-check insights between the expert interviews and the document data, and vice versa particularly in the context of EUDIW implementation in Estonia and Belgium.

The thematic analysis of the expert interviews was deliberately designed to build upon the preliminary findings from the document analysis. By first analyzing the literature and official documents published by the EU institutions, this research established an empirical and theoretical baseline that informed the design of the interview guide, the initial coding framework, and subsequent analytical focus. This sequence enabled a structured complementation and comparison between the official documents and expert interpretations, strengthening the triangulation of data sources.

As mentioned earlier in the document analysis section of this chapter, while the document analysis focused on semantic themes, in other words what the EU institutions and regulations explicitly state, the analysis of expert interviews adopted a latent thematic approach. This allowed for a deeper exploration of the underlying meanings, assumptions, and discourses shaping expert perspectives. In this way, by following inductive-deductive hybrid analysis, the research aimed to critically interpret how experts frame, problematize, or challenge the European Digital Identity Wallet requirements published by the EU and implementation of the EUDIW, going beyond surface-level meanings. By taking Kallio et al.'s (2016) guidelines as an example, the expert interviews consisted of four steps, namely, selection of interviews, interview preparation, conducting interviews, and thematic analysis.

4.3.1 Selection of Interviewees

Expert interviews aim to explore and collect data about a specific field of interest (Döringer, 2021). Meuser and Nagel (2009) define the expert interview as a qualitative, topic-guided interview focusing on the expert's knowledge which is a specialized expertise in a specific field of action. The criteria for being named as an expert, or the considerations for being recognized as a good or bad expert is subjective (Gläser & Laudel, 2009). Thus, for consistency and clarification, within the scope of this research, Döringer's (2021) expert definition is adopted. Döringer (2021) defines experts as knowledgeable individuals in particular subject and they are identified by virtue of their specific knowledge, their community position, or their status. In light of this definition, a person is considered an expert if they possess knowledge of digital identity or digital identity wallet within the context of this study.

In this context, since this research focuses on the actors and stakeholders involved in the implementation of the EUDI Wallet, representatives from various stakeholder groups in the Estonian and Belgian ecosystems were invited for interviews. These stakeholders consisted of issuers, ID Wallet providers, relying parties, ecosystem service providers, and private sector trust service providers ensuring a comprehensive and balanced perspective on the implementation process.

To ensure a comprehensive and diverse range of expert perspectives, a combination of purposive sampling and the snowballing techniques were used. Similar to the document selection process, purposive sampling in expert interview method have been utilized to select experts that are most likely to yield relevant and useful information (Campbell et al., 2020). In the context of this research, the aim was to increase the depth of understanding of the European Digital Identity Wallet implementation in Estonia and Belgium by selecting of experts based on their knowledge, experience, and relevance to the research topic.

Additionally, snowball sampling enabled the identification of additional key informants through referrals from initial interviewees, helping to capture a broader range of insights from other involved stakeholders. The method is particularly useful when the study is on a relatively private matter and requires the knowledge of insiders to locate people for the research (Biernacki & Waldorf, 1981). Even though the European Digital Identity Wallet is not a sensitive or private matter, it is still under development in many EU Member States if not all and some features, actors involved, and the roles taken by them are yet to be finalized. Therefore, to reach relevant, involved and informed stakeholders snowball sampling was used in this research.

As a result of purposive and snowball sampling in total of 56 experts from Estonia and Belgium from various organizations have been reached via cold emailing technique starting from 3 April Thursday 2025, until 28 April Monday 2025. As a result of these emails, 10 in-depth, semi-structured expert interviews were conducted with 14 experts, 8 of which from Belgium and 6 of which are from Estonia across various organizations. Experts were selected based on their stakeholder group affiliation to ensure representation of the various actors and stakeholders involved in the implementation of the European Digital Identity Wallet in Estonia and Belgium.

4.3.2 Interview Preparation

The format and guideline for the expert interviews were developed in accordance with the two primary functions of the interviews in this research. First, to complement the data extracted from document analysis and second, to elicit expert perspectives on key thematic areas. Semi-structured interviews were selected as a suitable method for this research due to their balance between flexibility and comparability (Kallio et al., 2016). As mentioned earlier, the European Digital Identity Wallet is still under development in many EU Member states. Even though the implementation acts and guidelines are being published by the European Commission, implementation and involved actors vary from one country to another. Additionally, even within the same country perceived drivers and barriers differ from one stakeholder to another. Given these reasons, semi-structured interviews allowed maintenance of a consistent structure across interviews while adapting to the expertise and responses of each participant. As Kallio et al. (2016) emphasize, semi-structured interviews support the use of follow-up questions and accommodate open-ended responses which enables rich and in-depth data collection.

Interviews were scheduled for approximately one hour to allow sufficient time for experts to elaborate on complex topics while maintaining focus. The interview guideline was developed in line with recommendations from Kallio et al. (2016) to ensure a coherent structure while ensuring flexibility. The initial set of questions was derived from academic literature, chosen theoretical framework, namely ANT and PESTEL, as well as preliminary findings from the document analysis. The interview questions were aligned with the main research question and its sub-questions to ensure methodological alignment and data relevance.

In this context, the interview guide consisted of an introduction and conclusion section, both standardized across all interviews, as well as four main thematic areas addressing the research questions of this study, particularly, first, the national digital identity wallet ecosystem and its stakeholders; second, the drivers for stakeholders in wallet implementation; third, the perceived barriers; and lastly, the lessons learned to date,

including implications for EU-level rollout. At the end of each interview, participants were invited to suggest additional relevant contacts who could provide complementary perspectives on the topic, particularly from other involved stakeholder groups. This snowball sampling strategy aimed to enhance the diversity and comprehensiveness of expert insights gathered during the study (Biernacki & Waldorf, 1981).

Given the exploratory nature of the study, the guideline was refined iteratively during the interview phase. Minor adjustments were made to adapt to the interviewees' professional background, context of either Belgium or Estonia, and domain expertise. However, the core structure of the guide remained consistent throughout the process. Where necessary, questions were rephrased or omitted, and clarifying or follow-up questions were introduced during the interviews to better explore the emerging issues.

Prior to interviews, a pilot test of the interview guide was conducted in order to assess the coverage and relevance of the content of the formulated guideline by using internal testing technique as described by Kallio et al. (2016). In line with this technique, the preliminary interview guide was assessed by the researcher's supervisor. Afterwards, received feedback was used to fine-tune the wording and sequencing of questions. Lastly, the interview guide was shared with experts in advance upon their request to enhance transparency and allow for informed preparation. Ethical standards were upheld throughout the research process by informing participants about how their data would be collected, used, anonymized, and deleted following its integration into the study's findings.

4.3.3 Conducting Interviews

Interviews were conducted digitally through a video conference on Microsoft Teams between April 3 and April 30, 2025, aligning with Kallio et al.'s (2016) guidelines on qualitative semi-structured interviews emphasizing context-sensitivity, dialogue, and flexibility. In line with the interview guideline, the interviews started with a brief introduction by the researcher, who introduced himself and provided an overview of the research background and objectives. The researcher then asked for the expert's consent to record and transcribe the interview in the Microsoft Teams environment, explaining that recordings would be used solely for scientific purposes including data analysis and validation.

Upon receiving consent and starting the recording, the experts were asked to introduce themselves and describe their roles within the organizations they represent. Afterwards, the interview proceeded following the interview guide which covered questions regarding the national digital identity wallet ecosystem and its stakeholders; second, the drivers for

stakeholders in wallet implementation; third, the perceived barriers; and lastly, the lessons learned to date, including implications for EU-level rollout, all of which were intended to address the research question and sub-questions.

Depending on the expert's professional background, associated organization and country, and the flow of conversation, the emphasis placed on each of the four main segments of the interview guideline changed. This adaptive questioning strategy ensured the balance between structure and flexibility (Döringer, 2021; Kallio et al., 2016). At the end of each interview, participants were invited to ask questions, clarify any issues, or elaborate on specific topics. They were also asked to recommend additional individuals who could offer complementary stakeholder perspectives.

A total of 10 interviews were conducted with 14 experts. Even though the experts were invited individually, some joined the interview with colleagues from their organization, resulting in three of the 10 interviews, namely interviews E102, E103, and B104, being group interviews. All of the interviews were conducted in English. As planned, the interviews remained within the predetermined time frame. Table 5 provides an anonymized overview of the interviews, including the experts' professional background, the dates on which they were conducted, as well as the duration of the interview in minutes.

As shown in the table, the expert sample fulfilled the intended diversity criteria with purposive sampling (Campbell et al., 2020). Experts representing all relevant stakeholder categories were interviewed, with at least one representative per stakeholder group from both Estonia and Belgium. Additionally, experts from private-sector trust service providers were also interviewed to capture the industry perspective on the European Digital Identity Wallet implementation in Estonia and Belgium even though they are not directly involved in the wallet implementation in their countries yet. This ensured a balance between perspectives from theory and practice as well as public and private sector, enabling a thorough and holistic understanding of the research topic.

Interview ID	**Professional Background of the Expert**	**Organization**	**Country**	**Date (DD/MM/YYYY)**	**Duration (minutes)**
E101	Digital Identity Risk and Compliance Expert	Cybernetica	Estonia	03/04/2025	62

E102	EU Digital Identity Wallet Field Manager Digital Identity Expert	Information System Authority (RIA)	Estonia	11/04/2025	61
E103	CEO eID and Trust Services Expert	SK ID Solutions	Estonia	21/04/2025	64
E104	Chief Digital Identity Officer	Ministry of Justice and Digital Affairs	Estonia	25/04/2025	62
B101	Information and Business Analysis Identification Authentication and Access Management	FPS Strategy and Support (BOSA)	Belgium	08/04/2025	57
B102	Programme Manager Digital Identity Wallet	FPS Strategy and Support (BOSA)	Belgium	14/04/2025	61
B103	Head of Risk and Compliance	itsme	Belgium	29/04/2025	71
B104	Deputy Director of Identity at Department IT Project Manager Project Manager for Digital Identity withing the Wallet	FPS Internal Affairs	Belgium	29/04/2025	56
B105	Legal Expert	FPS Economy	Belgium	30/04/2025	47
B106	Cybersecurity, Crypto and Certification Senior Advisor	Centre for Cyber Security Belgium	Belgium	30/04/2025	63

Table 5: List of interviews

4.3.4 Thematic Analysis of Interviews

Following the expert interviews, the research proceeded with the thematic analysis of the interview data. During this process, Naeem et al.'s (2023) guidelines on thematic analysis has been followed. After the transcription, phase 1, transcripts were reviewed for familiarization. During phase 2, initial codes were generated by identifying key recurring terms and patterns that reflected expert perceptions on stakeholder configurations, implementation drivers, and barriers. In phase 3, these patterns were coded using short labels that encapsulated the meaning of relevant textual units. Lastly, in phase 4 these codes were grouped into broader thematic categories that captured patterned responses across participants. At the end these themes were used to capture underlying meanings connected to the central and sub-research questions of this study on the European Digital Identity Wallet.

All interview recordings were transcribed while the interviews were being conducted except interview B104 since the experts did not give their consent for recording. For the other nine interviews, the automated transcription feature in Microsoft Teams was used. Therefore, detailed notes taken during the interview were used for the transcription of the session. A transcript was reconstructed from these notes, and any ambiguities were clarified with the experts via follow-up email to ensure accuracy.

The errors in the automated transcripts were manually corrected after rewatching the recordings. Additionally, timestamps were added during this process to facilitate accurate referencing and deeper analytical engagement in the results section. This iterative review facilitated familiarization with the data as well as reflection prior to coding. After the correction process, the transcripts were imported into MAXQDA, a qualitative data analysis software which allows structured coding, comparison, and interpretation of textual data.

As mentioned earlier in the thematic analysis of documents, both interview and documentary data were analyzed in parallel to facilitate effective triangulation and enable the identification of shared or divergent themes across sources (Bowen, 2009). An initial set of codes was generated based on the ANT and PESTEL theoretical frameworks, relevant literature, as well as the official documents after transcribing the interviews. This deductive structure provided a foundation, but the coding remained open to inductive insights emerging from interview data. As a result, some codes were expanded, redefined, or newly generated based on novel insights from the interviews, reflecting the hybrid, namely inductive-deductive analysis (Fereday & Muir-Cochrane, 2006).

Thematic patterns identified in the interview data were iteratively compared with the document themes to identify areas of thematic alignment, contradiction, or national as well as organizational specificity. These comparisons were utilized both as a form of cross-validation and as a means of revealing interpretive tensions such as differing stakeholder framings of the same technological feature enriching the thematic interpretation. Additionally, latent, in other words, interpretive thematic analysis was applied to uncover underlying assumptions, power dynamics, and discursive patterns in expert responses.

After deductively identified codes were grouped into tentative themes reflecting the evolving data, thematic refinement continued in the analysis of expert interviews, allowing for deeper insight and cross-validation between institutional and expert perspectives. To ensure effective triangulation, both data sets were analyzed together, allowing themes to emerge across the entire corpus (Bowen, 2009). This process ensured the sound implementation of inductive-deductive hybrid analysis.

Building on the themes and sub-themes derived deductively, the final thematic structure consisted of four main themes, namely, Institutional Roles and Ecosystem Definitions, Regulatory and Technical Foundations, Political and Legal Drivers, and Barriers to Interoperability and Implementation, and sixteen sub-themes. The former two themes, Institutional Roles and Ecosystem Definitions and Regulatory and Technical Foundations were composed of six sub-themes, all of which were identified deductively based on the existing literature, the Actor-Network Theory and PESTEL theoretical frameworks, as well as the document analysis.

Whereas the latter two themes Political and Legal Drivers as well as Barriers to Interoperability and Implementation were further refined into ten sub-themes, six of which resulted inductively from the interview data. These inductively developed sub-themes included, for example, the tension between national governance structures, the role of ministerial turnover in delaying implementation, the burden of lifecycle management in wallet use, and the emerging importance of killer use cases such as mobile driving licenses and age verification attestations. This way, a thematic analysis was performed for the entire data set with an inductive-deductive hybrid approach. As a result, this process established the foundation for the finalized results of this research, enabling the integration of expert stakeholder insight with regulatory, technical, and strategic dimensions outlined in official EU documents.

4.4 Limitations of Methodology

Even though the research employed a robust qualitative design combining semi-structured expert interviews with thematic document analysis, four methodological limitations should be acknowledged. These limitations do not undermine the validity of the findings but highlight the need for critical reflection on scope, representativeness, and the interpretive nature of qualitative inquiry. Therefore, future research may address these constraints.

First, expert interviews bring potential bias in representation and interpretation. Even though care was taken to include a diverse range of stakeholders across public and private sectors by using purposive sampling technique, the expert perspectives are shaped by their professional roles, strategic interests, and individual experiences. Additionally, upon experts' request, three of ten interviews were conducted as group interviews which may have constrained critical viewpoints or fostered conformity in responses.

Second, similarly, despite efforts to balance stakeholder representation, some stakeholder groups especially those who are not formally involved in decision-making process or those operating at the margins of implementation efforts remained underrepresented. In other words, the stakeholders who are actively involved are represented in the research while grassroots perspectives such as end user or citizen perspectives of the wallet remained underrepresented.

Third, even though the objectivity of data analysis tried to be ensured by utilizing triangulation of expert interviews and document analysis as well as by utilizing a hybrid deductive–inductive approach for the thematic analysis, the coding and theme development processes are not free from the researcher's theoretical lens and assumptions. In other words, while the use of qualitative software MAXQDA and iterative triangulation with document data enhanced analytical rigor, complete objectivity in qualitative interpretation is difficult to achieve.

Lastly, the document analysis is constrained by the availability and transparency of institutional publications (H. Morgan, 2022). The documents often reflect formal policy discourse and may obscure internal debates, conflicts, or implementation challenges. Even though the documents were crucial as a complementary source to expert interviews, document analysis is not free from methodological constraints.

5 Results

This chapter presents the empirical findings of the study, offering a comparative analysis of the emerging European Digital Identity Wallet ecosystems in Estonia and Belgium. Based on expert interviews, institutional documents, and the theoretical frameworks introduced in earlier chapters, particularly Actor-Network Theory and the PESTEL lens, the chapter maps the configurations of actors, infrastructures, and institutional logics that shape the rollout of the wallet in both national contexts.

Estonia and Belgium were selected not only for their contrasting governance models, namely centralized versus federated but also for their differing trajectories in digital identity innovation. Estonia offers a context of strong digital statehood and centralized technical capacity, while Belgium reveals a more fragmented but pragmatically adaptive ecosystem shaped by historical compromises and multi-level negotiations.

The chapter proceeds by analyzing each country separately, beginning with a detailed mapping of the wallet ecosystem, distinguishing between human and non-human actors. It then highlights the drivers and barriers influencing implementation through the PESTEL framework, identifying political, economic, social, technological, and legal dynamics. Lastly, each case closes with an assessment of national implementation strategies and the broader lessons that can inform the EU-wide deployment of the EUDI Wallet.

5.1 Estonia

5.1.1 EUDI Wallet Ecosystem in Estonia

The Estonian EUDI Wallet initiative is shaped by a heterogeneous and evolving network of actors whose interactions reflect a distributed but deeply interdependent ecosystem. This ecosystem is predominantly composed of public institutions, although the involvement of private stakeholders is expected to grow as the initiative matures. The actor configuration in Estonia is not fixed. Instead, it is marked by shifting responsibilities, blurred institutional boundaries, and ongoing negotiations, especially among state actors managing implementation.

Drawing on Actor-Network Theory (ANT), this section examines how human and non-human actors co-construct the EUDI Wallet ecosystem, with particular focus on the emergent roles, authority structures, and socio-technical alignments. In addition to ANT, the analytical categorization draws on the institutional role typology provided in the European Commission’s Common Union Toolbox.

The actor-network in Estonia can be divided into two broad categories. First, human actors and institutional roles, including ministries and public agencies, as well as selected private sector stakeholders from Estonia's established eID ecosystem. Second, non-human actors, including the eIDAS 2.0 regulation, the Digital Identity Wallet itself, PID datasets, national registries, and emerging certification frameworks all of which play active, structuring roles in the ecosystem.

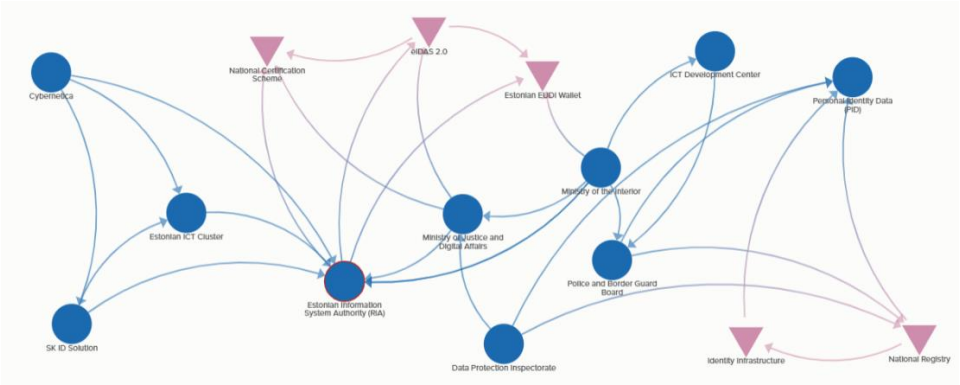

Figure 1: Illustration of Estonian European Digital Identity Wallet Ecosystem

5.1.1.1 Human Actors and Institutional Roles

The central human and institutional actors in the Estonian EUDI Wallet ecosystem are clustered around two ministerial domains, namely the Ministry of Justice and Digital Affairs and the Ministry of the Interior, each of which delegates operational responsibilities to subordinate agencies.

The Ministry of Justice and Digital Affairs serves as the lead institution responsible for implementing eIDAS 2.0 and establishing the national certification scheme. According to one senior official, "For now, for the development phase, it is decided that certification will be in the ministry. Currently, we do not have sufficient knowledge. This is why we are building knowledge within the ministry. However, later in the operating phase we may move it to another authority" (personal communication, April 25, 2025).

However, the ministry's involvement is primarily strategic. Operational authority is delegated to the Estonian Information System Authority (RIA), which is emerging as a pivotal actor in both technical implementation and regulatory interpretation. RIA is responsible for procuring the wallet solution, supervising trust services, and translating eIDAS 2.0 roles into Estonia's legal and institutional context. As one expert put it "RIA actually gets a completely new role. We have been more on the consultancy side... more on the software side, providing a supportive role before with the eID. We become much

more involved in the wallet; we are going to procure the solution" (personal communication, April 11, 2025).

Moreover, RIA's cybersecurity division extends its role to compliance and trust service supervision. While not formally responsible for the eID system itself, RIA will oversee wallet-related trust services through this division. One official clarified: "There is the information system and then there is the cyber part… under the cyber domain, there is also the supervision of trust services, and supervision of the wallet will be under there as well" (personal communication, April 25, 2025). These layered responsibilities suggest a distributed agency within RIA, where different subunits negotiate internally to align with the evolving wallet infrastructure.

Parallel to RIA's role, the Ministry of the Interior, along with its subordinate agencies the Police and Border Guard Board and the ICT and Development Center manages Estonia's foundational identity infrastructure. The Police and Border Guard Board is the legal custodian of the Personal Identity Dataset (PID) and plays a crucial role in issuing foundational credentials. One interviewee explained "Their main role is the provision of the PID and PID dataset because they are the owners of the personal data" (personal communication, April 2025). Meanwhile, the ICT and Development Center functions as an ICT service provider for both the Ministry of the Interior and the Police and Border Guard Board.

Other stakeholders include the Data Protection Office, responsible for regulatory oversight in data handling, as well as citizens, service providers, and relying parties, which is the entities that issue or request attestations. Although not yet fully engaged, these user groups will ultimately be responsible for validating the wallet's utility and legitimacy. Private actors including SK ID Solutions, Cybernetica, and members of the Estonian ICT Cluster maintain influence through their legacy systems, technical expertise, and advisory roles. While currently peripheral, these actors are expected to take on a greater role in implementation, particularly around technical integration and service delivery.

5.1.1.2 Non-Human Actors: Laws, Standards, and Infrastructure

In line with Actor-Network Theory, non-human actors such as regulatory texts, digital artifacts, and technical standards are not neutral backdrops but active participants in shaping the EUDI Wallet ecosystem. At the center is the eIDAS 2.0 Regulation, which functions as both a legal mandate and a structuring device. It defines institutional responsibilities and technical standards while forcing national actors to reinterpret existing boundaries. As one interviewee noted, "The roles are determined by the eIDAS

2 regulation… RIA is working on how to translate and interpret the regulation into the Estonian ecosystem" (personal communication, April 2025).

The EUDI Wallet itself functions as an obligatory passage point. It is a socio-technical artifact that integrates legal expectations, technical standards, and political agendas. The wallet imposes technical constraints such as attestation structure, mobile compatibility. Furthermore, it shapes legal and supervisory arrangements and demands institutional realignment. The wallet is bridging technical, legal, and political domains. It embodies EU-level requirements while needing to fit into Estonia's existing digital ID infrastructure. Its development compels state actors to make decisions about supervision, certification, and liability before many of these frameworks have been finalized.

In addition, technical artifacts such as the PID dataset, the national registry, and emerging certification schemes are elements that circulate across institutions while carrying stable authority. These components not only determine what tasks are performed, but also who is authorized to perform them, reinforcing or disrupting institutional boundaries.

5.1.2 Drivers and Barriers in the Estonian EUDI Wallet Ecosystem

5.1.2.1 Political Drivers and Barriers

Political dynamics play a pivotal role in shaping stakeholder engagement with the EUDI Wallet in Estonia. While there is a clear top-down mandate from the European Commission through eIDAS 2.0, strong governmental ambition and structural challenges impact the implementation landscape.

On the driver side, Estonia's historical leadership in digital governance and its participation in EU-wide pilot programs accelerate Estonia's action in the wallet adoption and implementation. By participating EU-led large scale pilot projects to test use cases before the wallet's roll out as well as aligning its national infrastructure with cross-border goals, Estonia is motivated to remain at the forefront of EU digital identity initiatives. "Estonia is part of the large-scale pilots such as Potential and EWC, so we have this kind of pressure to actually show something already in the spring" (personal communication, April 11, 2025).

Another key political drive is digital sovereignty and resilience. As experts during interview E102 explained "We are legally bound to have at least two state-provided, high-level eID means… used in different technological platforms" (personal communication, April 11, 2025). The motivation behind this is the fact that political desire to ensure Estonia is not dependent on any single system, especially considering the fact that

Estonia's digital service coverage is 100%, there should be a separate back up technological platform enabling Estonian citizens to reach to digital services and switch between different eID solution in case of need or any potential technical failures since some services are not available in any other format so falling back on paper format is not an option.

However, these drives are accompanied by barriers. Among the interviewees, a key recurring theme was the lack of internal clarity within the government regarding institutional roles. Several interviewees described the difficulty of assigning implementation and supervisory responsibilities. "We still are lacking the clarity of the roles within the government. Which ministry will be responsible for what in the EU wallet ecosystem?" (personal communication, April 21, 2025).

The uncertainty of responsibility ownership by the stakeholders is exacerbated by the tight EU timelines, which force national bodies to make strategic decisions before relevant legislation and technical specifications are finalized. "We have a deadline, but we do not have all the implementing acts that say how to do it. Only nine of the forty implementing acts have been published so far" (personal communication, April 25, 2025).

Especially from the ICT cluster perspective it has been stated that there is a heavy political pressure to show some success quickly. However, this political pressure to deliver visible success will lead to misalignment between long-term strategy and short-term implementation efforts.

5.1.2.2 Economic Drivers and Barriers

Estonia faces a double-edged reality in its EUDI Wallet implementation from an economic standpoint. While there are long-term strategic and economic benefits, the short-term costs and lack of convincing use cases present obstacles to broad engagement and adoption. One of the key economic drivers is the promise of cross-border data interoperability, which could streamline economic activity across the Baltic and Nordic regions as well as the entire European Union. "The biggest winning point would be the cross-border usability… that we could actually authenticate ourselves, sign digitally, exchange data across borders" (personal communication, April 25, 2025).

Given Estonia's mature eID ecosystem as well as position in the EU as one of the pioneers in digital infrastructure, stakeholders were concerned about the limited internal economic incentive for Estonia itself. Even though legally there should be at least two different alternative national eID tools and the wallet is seen as a backup digital identity infrastructure for the maintenance of the public and private sector digital services, among

the experts there was a shared concern about the potential redundancy of the wallet given Estonia's already functioning and mature eID ecosystem. Interviewees described uncertainty about the value proposition of building the wallet as something new that essentially duplicates existing services. Unlike some other EU Member States, Estonia already has a mature eID ecosystems, which already provides the wallet's promised core functions. "We have solved the question of authentication, digital signature, and data movement... So for us the question what do we have to gain from it still remains" (personal communication, April 25, 2025).

Additionally, from a cost-benefit perspective, the wallet is seen as a large expenditure with uncertain domestic returns. The experts representing the ICT cluster stated that "We simply see the wallet as something that is going to take attention and money from the existing ecosystems which is already working quite well" (personal communication, April 21, 2025). Similarly, another expert stated that "The wallet is a huge expenditure. It is a huge investment. It is a huge innovation… but for Estonia, it is kind of a step back. We do not know how to monetize it" (personal communication, April 25, 2025).

In line with these barriers, experts also stated that a major economic driver would be private sector participation, especially from the financial and service industries. Without commercial integration, stakeholders are concerned that the wallet will not reach everyday use relevance. "From an economic point of view for the wallet to fly, there have to be good use cases. There has to be uptake from the users, and that will only happen if the private sector is involved" (personal communication, April 25, 2025).

5.1.2.3 Social Drivers and Barriers

Social factors influencing the implementation of the EUDIW in Estonia affected both by the country's high level of digital literacy and the challenge of exceeding user expectations in an already advanced eID ecosystem.

Estonians are used to seamless digital government services. Therefore, Estonia's strong existing digital culture creates a paradox. Users already have tools that work well. This results in skepticism about the added value of the wallet. Any new solution must be as good as the existing solutions if not outperforming them. As one expert noted, the wallet does not generate a "wow effect" in Estonia compared to other countries where digital ID systems are less developed. "The wallet will not bring such a wow effect as maybe in some other countries. But we definitely try to attract users with features they may benefit from" (personal communication, April 11, 2025).

Therefore, there is a risk that the wallet will be perceived as redundant by citizens who already use authentication services via Mobile-ID and Smart-ID for daily authentication and e-services. “Estonian users are quite used to everything being simple… eID tools are available and working very well” (personal communication, April 11, 2025). Hence, users may perceive the wallet as unnecessary or redundant unless its advantages such as portability or cross-border utility are clearly demonstrated.

There is also concern about digital fatigue or confusion if the government introduces another identity tool without clear communication or support. “We do not want to end up with too many tools doing the same thing. It is confusing” (personal communication, April 11, 2025). These barriers could significantly hinder user adoption and slow down institutional enthusiasm to invest in deployment or outreach.

However, the social value of the wallet becomes clearer when the access to cross-border services taken into account. Cross-border mobility emerged as a practical and socially relevant driver for EUDIW adoption. In regions like the Baltics and the Nordics, citizens frequently travel across borders, often without carrying physical documents. The wallet’s ability to store verifiable digital attestations such as driving licenses was seen as a solution to common, real-world issues. “Having driving license attestations in the wallet would make it easier for citizens to move freely across borders. Very often, people forget their driver license when they go to Latvia or Helsinki. With the wallet, police in those countries could verify it digitally” (personal communication, April 11, 2025).

Cross-border advantages position the wallet as a citizen convenience enhancer rather than replacing existing tools, but for extending their usability beyond Estonia. Moreover, the potential for cross-border use of credentials and digital attestations is seen as highly valuable by both institutions and users. “Imagine being able to prove your degree to a university abroad from your phone. That is powerful” (personal communication, April 3, 2025).

A structural social barrier lies in the availability of experts in the ecosystem. The human capital required to develop, implement, and maintain the wallet is scarce in Estonia. The system requires specialized architects and engineers, of which there are very few “I can count people with this expertise on one or maybe two hands in Estonia” (personal communication, April 11, 2025). This skills gap impacts the social system's capacity to support and adapt to the wallet over time, particularly as user expectations grow and system complexity increases.

5.1.2.4 Technological Drivers and Barriers

Technologically, Estonia has a strong position. Its digital architecture including X-Road, Smart-ID, and Mobile-ID is mature and internationally recognized. Stakeholders expressed confidence in Estonia's ability to lead in digital infrastructure and standardization. "We already use digital identity means daily and we want to use it with others. That is the goal" (personal communication, April 3, 2025). In this context, Estonia's familiarity with mobile-first identity systems is also seen as an advantage. "Everything we do today is with the phone, so mobile readiness is there" (personal communication, April 25, 2025).

However, these strengths are also the origins of the barriers. The wallet requires building a parallel infrastructure, especially for handling attestations, which are conceptually and technically different from existing methods of data verification. The transition requires redesigning service flows across public and private systems. "We have to build a parallel system… rebuilding all services to accept attestations" (personal communication, April 25, 2025).

Cybersecurity was another concern, particularly around the EU's planned shared open-source codebase. "A single vulnerability in such a code is like an inherent threat to the whole ecosystem" (personal communication, April 21, 2025).

Finally, a lack of technical documentation and specifications during early phases made it difficult for stakeholders to prepare properly. "It is hard to build something when the technical specifications and standards, the specs are changing all the time" (personal communication, April 11, 2025). These issues reduce engagement by making technical actors, especially from the private sector hesitant to commit to solutions that may later need significant modification or rework.

5.1.2.5 Environmental Drivers and Barriers

In the Estonian context, none of the interviewed stakeholders referenced environmental factors in relation to the development or implementation of the European Digital Identity Wallet. Discussions consistently centered on legal, technical, and institutional concerns, suggesting that ecological sustainability is not currently part of the strategic vocabulary surrounding Estonia's digital identity ecosystem. This omission does not indicate irrelevance but rather a thematic gap in stakeholder priorities at this stage. The absence of environmental discourse in Estonia's EUDIW implementation is analytically significant and is further explored in the Discussion chapter.

5.1.2.6 Legal Drivers and Barriers

The legal requirement under eIDAS 2.0 obliging Member States to provide a digital identity wallet and ensure its interoperability across borders is the most clear-cut driver that all stakeholders stated. However, Estonia faces serious legal barriers due to the lack of finalized implementing acts, a missing national certification body, and ongoing ambiguity about supervisory responsibilities. These legal gaps create bottlenecks in planning and procurement. “Even if Estonia has the wallet now, it will not be able to certify it” (personal communication, April 3, 2025).

Stakeholders also expressed their concern regarding the incomplete legal foundation and implementing acts. “We are expected to be ready without the legislation telling us how” (personal communication, April 25, 2025).

Legal barriers extend to internal conflicts about authority. Estonia lacks clarity on who should serve as the supervisory authority for wallet trust services, and concerns were raised about conflicts of interest. An expert from the Estonian Public Administration stated that “It is not ideal that the same authority is involved in both implementing and supervising the wallet” (personal communication, April 25, 2025).

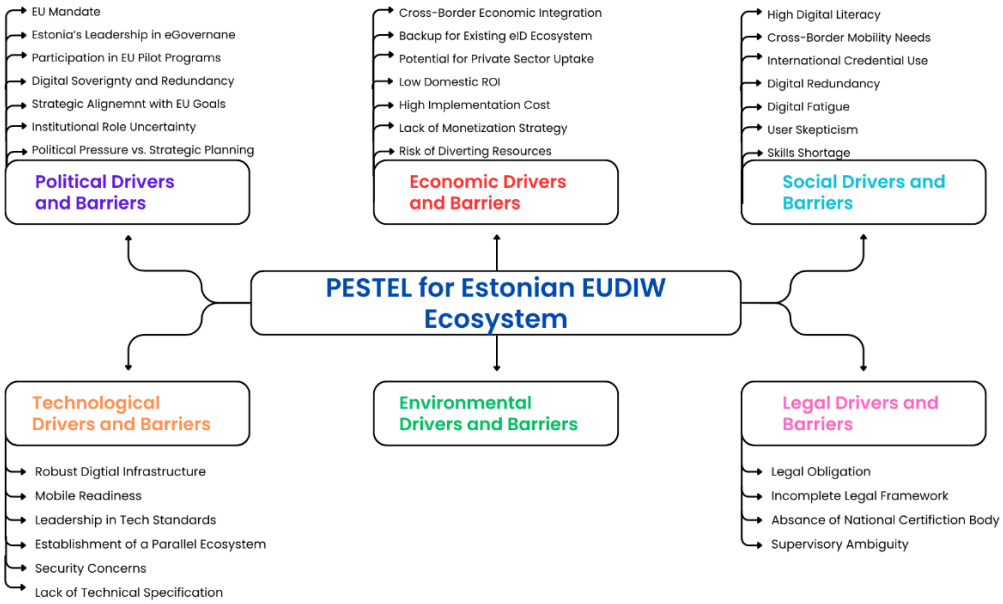

Figure 2: PESTEL for Estonian EUDIW Ecosystem

5.1.3 Estonia’s EUDIW Implementation Strategies and Lessons for the EU Rollout

Estonia’s EUDI Wallet implementation reflects a high degree of digital maturity, combined with a cautious yet pragmatic strategy shaped by legal ambiguity, resource

constraints, and a strong commitment to public-private collaboration. Despite Estonia's leadership in digital governance, the EUDI Wallet rollout has presented challenges that underscore the limitations due to unclear regulation, evolving technical specifications, and EU-wide interoperability demands. At the same time, Estonia offers a set of nuanced lessons that could inform a more effective and coordinated European implementation.

5.1.3.1 National Implementation Strategy

Estonia's EUDIW strategy is centered around leveraging private sector capabilities while maintaining strong state oversight. Unlike some Member States developing a government-built wallet, Estonia has explicitly opted for a procurement-based model. "We are not going to develop the solution ourselves," explained experts from RIA. "We are looking for the best and most suitable solution from the market. The goal is to ensure technical flexibility, stimulate innovation, and avoid duplication of existing solutions, such as the mobile-ID and eID systems already in use. The wallet, in this model, will be provided as a service by private vendors, with the state acting as issuer and RIA managing critical integrations" (personal communication, April 25, 2025).

The implementation has been marked by role complexity and internal governance challenges. RIA, which is both the procuring authority and a supervisory agency under a different department, must manage potential conflicts. "We are representing the eID department… the supervisory authority is actually a different department, but in the same organization," noted one RIA official, reflecting concerns about perceived neutrality (personal communication, April 11, 2025). Efforts have been made to preserve internal separation of roles, but the organizational overlap remains a delicate issue.

Estonia also faces gaps in institutional capacity, especially in certification and standardization. "Our technical supervisory authority does not have strong background knowledge about wallet certification," noted RIA official (personal communication, April 11, 2025). The absence of a national certification framework, in light of the delayed EU-wide certification scheme, leaves Estonia in a holding pattern, relying on incomplete guidance. According to one expert, "We put certification on hold… most countries do not have national schemes" (personal communication, April 3, 2025).

Moreover, the challenge of aligning domestic implementation with EU legislation is compounded by time pressure. As one respondent explained, "We are getting the finalized versions of the standards on the go, but at the same time, we already need to have the procurement out" (personal communication, April 11, 2025). This mismatch creates friction between compliance requirements and operational feasibility.

5.1.3.2 Key Lessons for the EU Rollout

Estonia's experience offers several key insights for the other EU Member States. First, there is a pressing need to synchronize regulatory development with implementation timelines. "It would have been better to have implementing acts ready together with eIDAS 2.0… or within six months. Now we are seeing delays of 12 to 24 months" mentioned an expert (personal communication, April 11, 2025). The asynchronous publication of implementing acts and technical standards creates legal and procedural bottlenecks at the national level.

Second, ce. RIA plays multiple roles in the EUDIW implementation, namely acting as the wallet issuer, managing key integration points like the eIDAS node, and overseeing procurement. While this centralization facilitates technical coordination, it also introduces challenges in maintaining clear boundaries between implementation and supervision. Estonia aims to mitigate such concerns by ensuring that wallet development is handled through open public procurement rather than in-house development. As an expert from the Estonian Ministry of Justice and Digital Affairs noted, "We want to support a free and open market… ideally several wallet offerings through procurement" (personal communication, April 25, 2025). This approach reinforces Estonia's longstanding preference for public-private cooperation while preserving institutional neutrality.

Third, Estonia emphasizes the critical role of strategic communication. According to RIA, successful implementation depends on "making sure all organizations' leaders understand the priority and have the resources to do things" (personal communication, April 11, 2025). This includes upstream engagement with public sector actors to adapt their processes, and downstream communication with citizens to ensure adoption. "We need a kind of carrot for the users," said one official, pointing to potential value-adds such as mobile driving licenses or age verification features (personal communication, April 25, 2025).

Fourth, there is a strong call for realistic expectations and modest framing. Several Estonian experts expressed skepticism about the viability of EU-wide interoperability within the proposed timeframe. "We have not managed digital signature interoperability in 25 years… and now we expect wallet interoperability in two years" (personal communication, April 21, 2025). This skepticism extends to the governance model, which some view as repeating past mistakes of overregulation without value creation. "We created business investment without business need," they added, giving GDPR's unintended burden on SMEs as an example (personal communication, April 21, 2025).

Fifth, the lack of a shared European certification scheme poses a major risk to trust and interoperability. As one stakeholder noted, “We have no idea whether the German Wallet users will trust the Spanish Wallet users. We need a common certification scheme. Without this, cross-border use remains more aspirational than operational” (personal communication, April 3, 2025).

Finally, Estonia’s experts warned of the mismatch between ambitious regulatory rhetoric and the complexity of real-world implementation. “User-friendliness cannot be mandated by regulation,” argued experts from SK ID Solutions (personal communication, April 21, 2025). “The reports are full of Commission-pleasing language but ignore things in plain sight”. Unless usability, liability, and business models are taken seriously, the wallet may struggle to attract either users or service providers (personal communication, April 21, 2025).

5.2 Belgium

5.2.1 EUDI Wallet Ecosystem in Belgium

The EUDI Wallet ecosystem in Belgium is shaped by a layered and federated institutional landscape, where responsibilities are distributed among several federal agencies, with limited but growing involvement from regional actors and the private sector. Unlike Estonia’s relatively centralized approach, Belgium’s ecosystem is coordinated by the Federal Public Service Policy and Support (BOSA), which serves as the designated wallet provider and leads both strategic and technical implementation. BOSA works in tandem with the FPS Interior, FPS Economy, the Center for Cybersecurity Belgium (CCB), and pre-existing infrastructures such as the Federal Authentication Service (FAS).

This section analyzes the co-evolution of human and non-human actors that constitute Belgium’s wallet ecosystem. Drawing on ANT and institutional typologies from the Common Union Toolbox, it maps how regulatory frameworks, digital platforms, identity data sources, and certification infrastructures shape actor roles and interactions. The result is a complex, evolving network where governance, compliance, and infrastructure are being realigned in response to eIDAS 2.0 and the technical demands of the MyGov.be wallet.

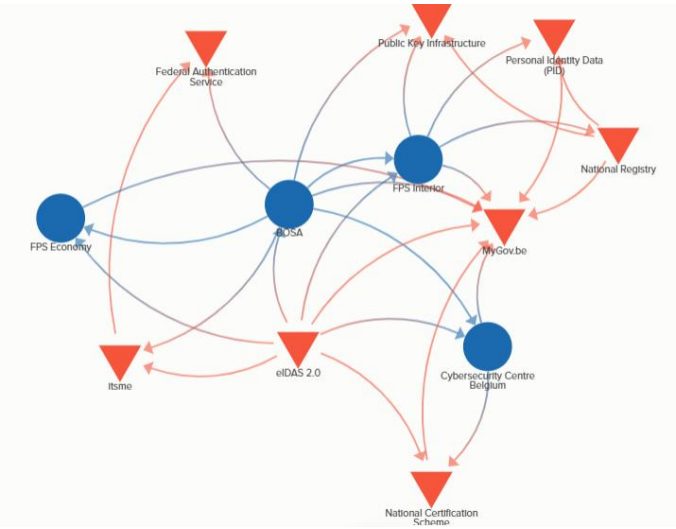

Figure 3: Illustration of Belgian European Digital Identity Wallet Ecosystem

5.2.1.1 Human Actors and Institutional Roles

In the Belgian EUDI Wallet ecosystem, Federal Public Service Policy and Support (BOSA) emerges as the central orchestrator of the technical and strategic implementation of the wallet. BOSA's role in eID is not new. BOSA has been in charge of the Federal Authentication Service (FAS) which provides authentication to 80% of Belgian citizens. Last year in 2024, FAS has offered almost 300 million authentication mainly to online public services and today almost 2000 online services use the FAS (personal communication, April 8, 2025).

As the government-designated wallet provider, BOSA is responsible for developing the MyGov.be application. An expert from BOSA explains "BOSA is in charge of the ID means and the authentication part of the wallet. BOSA will be the wallet provider and will remain as the provider in the future. The wallet is called MyGov.be. You can already download the app. Today it only allows authentication for some public services… but we are now working on the signature remote signing use case… and in the future we will support all kinds of electronic attestations of attributes" (personal communication, April 8, 2025).

In the EUDI Wallet ecosystem in Belgium, BOSA's leadership is being accompanied by other public bodies. The Federal Public Service of Interior (FPS Interior) plays a critical role as the authentic source of identity data. FPS Interior has the National Register which is the foundational database behind Personal Identification Data (PID) provision. The experts from FPS Interior stated that "We are responsible for identity in general, so we will be responsible for PID. We are not only fetching the data as the authentic source but

also defining and making sure business rules are respected regarding everything that comes to digital identity" (personal communication, April 8, 2025).

Given their roles the collaboration between FPS Interior and BOSA is more than data provision. It extends to co-management of the Public Key Infrastructure (PKI) infrastructure used for issuing signing certificates. "FPS Interior together with BOSA also manages the PKI… this is typically an example where we are co-responsible. We are not limited to being the authentic source, but we also decide together with BOSA all the business rules and treatments for the functionality added" (personal communication, April 29, 2025).

Federal Public Service Economy (FPS Economy) is another key public actor in the EUDI Wallet ecosystem in Belgium. Although its future involvement in wallet governance is still under discussion, the FPS Economy plays a regulatory and supervisory role, particularly for trust services. The expert from FPS Economy clarified that "We are the supervisory body of trust services for those providers that want to have the qualified label… We do have some experience when it comes to being a supervisory body of trust services. However, it is not set in stone yet who will be the supervisory body of the wallet" (personal communication, April 30, 2025).

The Center for Cybersecurity Belgium (CCB) as the national cybersecurity certification authority which is responsible for the wallet's conformity assessments is another key actor in the wallet ecosystem. "An eID wallet needs to be certified before you can use it as a European digital wallet. CCB is responsible for the certification scheme and the supervisory part of that" (personal communication, April 30, 2025).

Additionally, even though they are not fully integrated, regional governments, the Ministry of Mobility, Ministry of Health, and Ministry of Foreign Affairs are relevant actors for future attestations such as driving licences, vaccination certificates, and university degrees. "Regional level stakeholders are not yet a priority, but they will be in the future. For example, diplomas are governed by the Communities. These will be onboarded later" (personal communication, April 14, 2025).

Even though they are not involved in the wallet's development, itsme, a private sector identity provider legally recognized under a royal decree anticipates a strong integration in the lifecycle of identity provisioning. A representative emphasized the lack of involvement, while also noting the technical synergy. "You should know that we are not as such involved directly in the project. We have been asked to test the alpha product and do pilot testing… But we see this becoming a very tight integration. The way it works is already obvious for us… They will do an itsme authentication login… then they will push

the information into the mobile wallet infrastructure" (personal communication, April 29, 2025).

5.2.1.2 Non-Human Actors: Infrastructure, Legislation, and Platforms

Non-human actors in Belgium's EUDI Wallet ecosystem are essential to understanding how institutional relations are shaped and materialized. As the future wallet itself, MyGov.be app is a central actor by being a boundary object around which legal mandates, identity systems, and institutional responsibilities are coordinated. Currently, the app has already been launched, but not as a European digital wallet. It is only an authentication app with some extra functionality. It is a phased approach. First national and Euoprean Certifications of the app should be completed to be able the certified as an EUDI Wallet.

As another non-human/institutional actor, the National Register, managed by FPS Interior, operates as the authentic source for identity data. "The National Registry will be the authentic source on the PIDs, which will be used to render the wallet solid. It will also be the authentic source on all other attestations based on the data that's reading the national registry" (personal communication, April 29, 2025).

The PKI infrastructure is another critical non-human actor, as it enables digital signatures and identity assertions. According to the experts, co-managed by FPS Internal Affairs and BOSA, the PKI infrastructure is central to how digital signing will work in the wallet" (personal communication, April 29, 2025).

eIDAS 2.0 Regulation is another key non-human actor. The regulation has shifted previous institutional boundaries and impacted the digital wallet as well as identity ecosystems in Beligum. "With eIDAS version one, we had a clear separation between the ID means and trust services. Now with the wallet, the border is more blurred… we have electronic attestations that will also be trust services. We have to manage both". (personal communication, April 8, 2025).

The Certification Scheme as another key non-human actor is still under development both in the National Level by the CCB and the European Level by ENISA. The certifiacation scheme will determine who can issue wallets and under what security and legal conditions. "There is a whole system of accreditation. Audit companies need to be accredited by the National Accreditation Body. We, CCB, will create the certification scheme, and it will be approved and implemented in coordination with them" (personal communication, April 29, 2025).

The Federal Authentication Service (FAS), used by most Belgian eID users, is also deeply embedded in the architecture of identity and remains as backbone. "You can connect via

electronic identification card or via itsme. All the organizations who need authentication services today are our stakeholders" (personal communication, April 14, 2025).

5.2.2 Drivers and Barriers

5.2.2.1 Political Drivers and Barriers

Political dynamics in Belgium play a crucial role in shaping the implementation of the EUDI Wallet. On the one hand, political drivers include strategic alignment with EU sovereignty goals and governmental ambitions to enhance citizen control over digital identity. On the other hand, complex political climate, different priorities between ministries, and the complexity of Belgium's federal governance create barriers to the wallet implementation.

A major political driver for EUDI Wallet in Belgium originates from European Commission's ambitions to reduce dependency on non-European technology providers. As one expert stated it, "One of the key drivers for the Commission to initiate the wallet was to ensure internal European control of European citizens' data and not to leave the market to others" (personal communication, April 8, 2025). This drive for digital sovereignty is echoed at national levels. Another stakeholder reflected that "the Commission wants to be quick with the wallet, because Apple Wallet in the United States already connects with the mobile driving license. We have to have a European alternative" (personal communication, April 14, 2025).

In national level, the political narrative has emphasized increasing citizen control over personal data. "On the Belgian political level, there has been a government agreement to ensure that all citizens and organizations should receive more control over their own data… and online access to a number of government services… all integrated and accessible by the wallet" (personal communication, April 29, 2025). This narrative has helped frame the wallet not merely as a compliance tool, but as a transformative digital service for public administration.

Despite these drivers, political factors also create barriers for the EUDI Wallet implementation in Belgium. Belgium experienced a period of political vacuum following the Federal Elections on 9 June 2024, which significantly delayed decision-making made it unclear. "We have been with no government for eight months… which did not help to get a clear position from the political level" (personal communication, April 8, 2025). Even when governments are in place, communication and make the political actors understand the issue is challenging. "The wallet is a difficult concept to understand,

sometimes the understanding of problems does not align between us and the political actors" (personal communication, April 14, 2025).

Additionally, stakeholder coordination remains also challenging due to diverging responsibilities, objectives, and internal decision making and processes not only among different institutions but also among different governance levels as well. An expert gave an example from the interaction between BOSA and FPS Interior. "We want to go quicker, and the Ministry of Interior takes a bit more time because they want to think more about it. But maybe it is for good reason, because they are responsible for the identity of all Belgians" (personal communication, April 14, 2025).

Other political barriers include uncertainty about the governance of private wallet providers. "We still must see from a political level what will be the position regarding private wallet solutions… this will be a political decision" (personal communication, April 8, 2025). Intensified by Belgium's complex federal structure and need for both national and European coordination, political ambiguity slows down the alignment among stakeholders and results in a cautious, sometimes fragmented, implementation style. "Belgium has a complex governance structure. In wallet implementation we need to involve many partners from different levels whenever more partners are involved, decision making can be slowed down" (personal communication, April 30, 2025).

5.2.2.2 Economic Drivers and Barriers

Economically, the EUDIW is seen both as a modernization effort with long-term efficiency gains and as a costly undertaking that stretches human and financial capacities. The dual pressures of strategic opportunity and operational constraints define how stakeholders navigate their economic engagement.

The wallet initiative is framed as a cost-saving modernization tool. "The idea of the wallet is also to replace… several apps of the government. So this is efficiency… not spending three budgets for three different apps" (personal communication, April 14, 2025). It consolidates digital public services and avoids app fragmentation, offering both administrative and financial streamlining.

Private sector stakeholders also see opportunity in the EUDI Wallet. "It is an improved access, secure and privacy-friendly access to digital services accepted throughout Europe… banks and telcos will benefit from automation of their know-your-customer obligations" (personal communication, April 29, 2025). Especially for industries with cross-border customer bases, the wallet's standardization holds significant economic promise.

Additionally, the EUDI Wallet has potential to boost the digital economy further both within and across the EU Member States including for SMEs and startups. “Especially after COVID 19 businesses had to rethink their business models. I think there are still a lot to be done to boost the digital economy further especially the wallet is an opportunity to hop on the digitalization trains and stay there” (personal communication, April 30, 2025).

However, unresolved financial structures pose challenges. “The business model is not that clear… especially the liability and specific service level agreements (SLAs)” (personal communication, April 8, 2025). Many stakeholders express uncertainty about how costs, responsibilities, and risks will be distributed between public and private actors. Additionally, even though the wallet has to be usable by private services, the authentication service is not being offered to private sector or service providers yet. Therefore, the use of wallet by the private sector is still unknown.

Human resource and budgetary constraints further complicate implementation. “It is also very hard or complicated to find the adequate competencies… and we are not such a big team” (personal communication, April 8, 2025). In a similar vein, another expert argues that small member states like Belgium face difficulty scaling development to meet certification deadlines. “Certified solution is needed by the end of 2026 and many standards as well as documentations are missing. This requires a lot of resources, human resources, and a lot of experts. There are always the same experts working on them, not only for EIDAS but also for other legislation such as Cyber Resilience Act, NIS 2 and ICE 2. There are only 24 hours in one day” (personal communication, April 29, 2025).

Making the wallet fit into the existing eID ecosystem in Belgium is another challenge. The eID ecosystem in Belgium is in place for more than ten years and it needs to remain functional until the EUDI Wallet ecosystem becomes functional. “We are little bit worried about this because we work with very new things without being tested before. We invest a lot of money, a lot of resources, and a lot of time. We have to make sure that all these resources or the existing eIDAS ecosystem do not go to the dustbin” (personal communication, April 14, 2025).

In line with the potential conflict with the existing eID ecosystem, there are two main barriers. First, one of the experts argue that some competitors from the private sector might see the wallet as a threat for their solution since they perceive the wallet as something that will replace their solution (personal communication, April 14, 2025). Secondly, some actors from the private sector feel excluded from procurement or development processes, raising questions about transparency. “If they could just collaborate with the private companies for identification means… we could have been

much farther with this initiative. If you want to make this work as an ecosystem, you will have to take into account what a private sector wants from this" (personal communication, April 29, 2025).

There is also a discussion over how public funding is provided and being allocated. "It is not clear in the Belgian setup that currently under which grant, and budget is this being done. Coming back to Officialization of this initiative, there has been discussions about where and when were these funds attributed to the parties that are actually actively developing the code and the back-end infrastructure for this for this initiative" (personal communication, April 29, 2025).

5.2.2.3 Social Drivers and Barriers

EUDIW is envisioned as a socially transformative tool. "Simplification… the citizen does not have to use different tools… they have the information in their pocket, on their smartphone" (personal communication, April 14, 2025). This convenience is particularly meaningful for populations with limited access to computers. "Some people do not have a PC… for them, the wallet is a much better option" (personal communication, April 14, 2025).

Public trust is central. "We want to promote safety, trust, but also digital inclusion… and protection of consumers and businesses" (personal communication, April 30, 2025) Trust-building measures include designing transparent interfaces and enabling data minimization. "If people do not trust it… they are not going to use it. So, we try to work in a transparent way and not hurry things" (personal communication, April 29, 2025).

Creating an inclusive solution is another driver for the EUDI Wallet in Belgium. Successful implementation is not only about availability and use of the solution by tech savvy people. "90% of people are digitally autonomous knowing how to install the mobile apps and how they work. However, it is also about people that are less digitally savvy and including also them, including people that are less capable" (personal communication, April 29, 2025). Another expert added that "We want to make sure that digital services can be done in in an easy way. We want to include as many people as we can" (personal communication, April 30, 2025).

Despite these ambitions, stakeholders recognize the complexity of the wallet concept. "The concept itself of digital identity wallet… is quite complicated to understand… even some ministers thought the wallet was just a competitor to itsme" (personal communication, April 14, 2025). This confusion leads to friction, misinformation, and reduced buy-in across stakeholder groups. Additionally, from the end users' perspective,

the end users should be communicated and provided with clear information to show the benefits of the wallet to encourage use in comparison to existing solutions. “There are already other systems in place, so we will need to convince people through clear information and show the positive sides of what this wallet” (personal communication, April 30, 2025).

Digital literacy and divide remain a critical issue. The web tax declaration in Belgium started almost twenty years ago. Therefore, most of the Belgian citizens make use of their eID cards, itsme or other ID means for online services. However, the wallet will be a new product, and the concepts of attestations and attributes are not self-explanatory. “We will have to find a way not to ask people to consent on everything each time you want to take an action in the wallet, but it must remain easy to use and quite understandable and intelligible” (personal communication, April 8, 2025). Additionally, another expert added that “There are people who do not want to or cannot use a device… there must always be a non-digital alternative” (personal communication, April 14, 2025).

Surveillance and privacy concerns are another key social barrier for the EUDI Wallet implementation in Belgium. Although the eIDAS 2.0 regulation allows certain personal attributes to be shared with relying parties, the architecture must ensure that privacy is preserved throughout this process. To achieve this, an intermediary role is essential. This intermediary serves as a pivoting point, ensuring that relying parties can verify the validity and qualification of shared attributes without knowing their exact origin. Likewise, the issuing party should not be able to trace which relying party has accessed the information. This separation helps protect users' private lives and mitigates the risk of profiling. One expert emphasized the public's skepticism “There is a paranoia from certain sets of the population… they say, we do not trust it, it is coming from the government” (personal communication, April 29, 2025).

5.2.2.4 Technological Drivers and Barriers

Technological innovation is at the heart of Belgium’s EUDI Wallet initiative. The EUDI Wallet introduces a complex and innovative digital infrastructure. While new features such as mobile-based signing, cross-border compatibility, offline use promise progress, complexity of the system, evolving standards, technological immaturity and security concerns create friction across the stakeholder landscape.

Smartphone-centric architecture is one of the project’s greatest technological drivers. “A large portion of the population in Europe are used to running their apps running their smartphone as centerpiece of their daily life. So having every document necessary in digital format is a great use for people” (personal communication, April 29, 2025).

Furthermore, another interviewee highlights “With the wallet, people will be able to sign only with the smartphone… they do not need a card reader anymore” (personal communication, April 14, 2025). The move from hardware-based eID systems to flexible mobile apps significantly lowers barriers to access.

Technological convergence also enhances value. “One big win is the offline use case… for example, proving your identity to police forces offline via a QR code” (personal communication, April 29, 2025). Integration with banking and other private applications further strengthens the ecosystem “There will be organizations willing to integrate wallet support if SLAs are guaranteed” (personal communication, April 29, 2025).

An expert summarizes the one of the main drivers for the wallet as “The European Commission introduced the idea of the wallet to have a secure and reliable digital identification that works across the whole of Europe and that can compete with the already existing models that are being made by Google or Apple for the European Union’s digital sovereignty” (personal communication, April 30, 2025)

However, the technological ecosystem is far from stable. “We are missing some kind of beta product that really can be used to test… the timing is the problem” (personal communication, April 8, 2025). Stakeholders must navigate fragmented standards and immature components. “Some functionalities like unlinkability are not standardized and not available in 99% of phones” (personal communication, April 29, 2025).

Security is a pressing concern. “The app has to function in a hostile smartphone environment with many requirements and vulnerabilities” (personal communication, April 29, 2025). Given these security concerns and vulnerabilities, an expert emphasized that “It is important to have top level security and constant improvement of the app. The wallet should be a kind of fortress” (personal communication, April 14, 2025). Additionally, stakeholders are also skeptical about requirements to open-source code, which they argue undermines security (personal communication, April 14, 2025).

Another pressing technical barrier is interoperability and cross-border identification. “We have to make sure that all solutions are interoperable with other European systems” (personal communication, April 8, 2025). By highlighting the potential fraud vulnerabilities another expert argued “You have to match the PID you get from another country with local data… it is unclear which information is correct,” (personal communication, April 30, 2025). Additionally, uncertainty around final specifications further hampers development. “We are building something based on a moving target… with requirements still under negotiation,” (personal communication, April 29, 2025) complained one expert.

5.2.2.5 Environmental Drivers and Barriers

Similar to Estonia, in Belgium, environmental dimensions were entirely absent from the interviews with institutional actors and technical experts involved in the EUDIW ecosystem. This silence points to a broader pattern in which environmental sustainability is not yet embedded in the operational or policy discourse around digital identity wallet. As in the Estonian case, this analytical gap is addressed in greater depth in the Discussion chapter to highlight its implications within EU-level digital and sustainability frameworks.

5.2.2.6 Legal Drivers and Barriers

Legal forces are perhaps the most definitive factors impacting EUDI Wallet implementation in Belgium. The eIDAS 2.0 regulation provides clear mandates, but ambiguity in implementation acts, certification schemes, and timelines generates substantial legal risk and uncertainty for stakeholders.

Above all, legal obligation underpins the project. “It is a legal obligation to provide one wallet… that gives a boost to its adoption” (personal communication, April 29, 2025) Budget justifications for the project rely heavily on this framing as well. “We cannot ask more money for a new project when we are on limited budget unless it is a legal obligation… that was the most convincing argument for the EUDI Wallet establishment” (personal communication, April 14, 2025).

Legal harmonization is also valued. “Instead of having 27 different legislations, we now have at least a common framework” (personal communication, April 30, 2025). This fosters shared commitment across Member States and offers predictability for private actors functioning across different EU Member States.

The most pressing barrier that is highlighted by every expert is the tight and unrealistic deadline. The Member States are expected to deliver a certified wallet by the end of 2026. Therefore, they have eighteen months to comply with many elements that are not clear yet. “Conformity Assessment Bodies must put everything in its place to be able to deliver this new service on the market, to certify solution regarding a new scheme. This is almost impossible to do all this properly in the given timeline” (personal communication, April 14, 2025).

The regulatory environment remains deeply fragmented, posing another significant challenge to the EUDI Wallet’s implementation. One major issue is that many of the implementing acts which define the specific requirements the wallets must fulfill have yet to be published. As a result, the technical and operational expectations remain

uncertain. One of the experts explains it as “We have the eIDAS regulation, which sets out high-level requirements, but many critical details still need to be clarified. These specifications are being developed through batches of implementing regulations, which are still in progress” (personal communication, April 30, 2025)

Certification of the wallets brings another layer of challenge. Even though an EU-level certification scheme is being established by ENISA, until then each Member State must also develop its own national certification framework. Hence, the certification challenges are particularly acute. “Developing a national certification scheme takes time… and 18 months is nothing” (personal communication, April 8, 2025). The fragmented national schemes may also hinder future European-level alignment.

Legal-technical misalignment further complicates implementation. “The wallet is still a moving target… many specifications are not finalized” (personal communication, April 29, 2025). Similarly, another expert emphasized that “The specifications were seen as immature… we are building small pieces without knowing how they fit together” (personal communication, April 14, 2025). Implementers must build on unstable ground, hoping future legislation will not invalidate their designs.

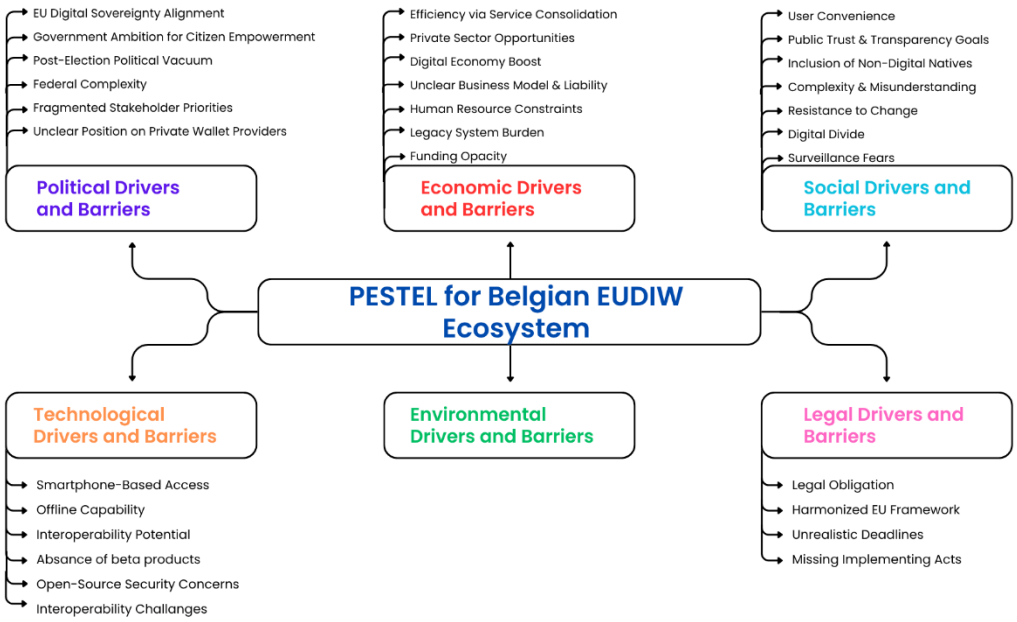

Figure 4: PESTEL for Belgian EUDIW Ecosystem

5.2.3 Belgium’s EUDI Wallet Implementation Strategies and Lessons for the EU Rollout

Belgium’s approach to implementing the European Digital Identity Wallet is marked by a cautious, phased, and highly collaborative strategy that reflects both the complexity of

the ecosystem and the ongoing evolution of European regulatory frameworks. Experts from public authorities, cybersecurity bodies, and private actors agree that while progress has been steady, many lessons have emerged about the timing, governance, and coordination necessary for successful implementation at both national and European levels.

5.2.3.1 National Implementation Strategy

Belgium's implementation strategy is characterized by three overarching principles, namely phased deployment model, stakeholder coordination as well consultation, and adherence to a strict role separation. The phased model ensures gradual feature development within the MyGov.be application. The app currently focuses on authentication for natural persons, and future iterations will incorporate legal person authentication and representation functionality once the regulatory landscape stabilizes. As explained by one BOSA official, "Today our wallet also focuses on the authentication for natural persons... and we will integrate the authentication of legal persons as soon as we have a clear view on how to do it" (personal communication, April 8, 2025). This cautious approach helps manage political and technical uncertainty while enabling early experimentation with concrete use cases, such as remote signing.

The Belgian government has also emphasized inclusive governance and multi-stakeholder consultation. "We always consult with national stakeholders to ensure there is consensus on our position towards the Commission," noted one expert (personal communication, April 8, 2025). However, internal coordination was challenging, particularly when political leadership was uncertain. As one official noted, "We were without a government for eight months… which does not help to get a clear position from the political level" (personal communication, April 8, 2025).

Segregation of responsibilities is another cornerstone of Belgium's strategy. As a CCB expert explained, "The agencies responsible for developing services like the wallet are completely separated from the supervisory bodies… we report to different ministries" (personal communication, April 30, 2025). This structure supports transparency and mitigates conflict of interest, with BOSA developing the wallet, the CCB handling cybersecurity and certification, and FPS Economy overseeing trust services. These roles are coordinated through three implementation tracks that are legal harmonization, certification scheme development, and technical supervision (personal communication, April 30, 2025).

5.2.3.2 Key Lessons for a broader EU Rollout

Belgium's experience yields several lessons for the broader European rollout. First, stakeholders unanimously point to the need for greater clarity and direction from the European Commission. "If you are a wallet provider, you need to know what to do to get your wallet approved. At this moment, it is not clear," highlighted a cybersecurity expert (personal communication, April 30, 2025). The lack of mature reference implementation has led to inefficiencies and ad hoc development. "Everyone worked in an ad hoc manner… we could not use what we were supposed to use" (personal communication, April 8, 2025).

Second, interviewees emphasized the importance of collaboration both within and across Member States. Belgium participates in a five-country alliance with France, Germany, Spain, and the Netherlands to jointly develop a reusable certification scheme. This cooperation fosters resource sharing and reduces the risk of fragmented solutions. "It is a European project, but it is dependent on what each Member State does. If there is a breach in one country, trust in the whole system suffers," underlined one expert (personal communication, April 30, 2025).

Third, Belgium's experience underscores the risks of premature development in the absence of legal certainty. "We spent a lot of time developing a prototype that may not be reusable. The standards keep changing," explained an expert from BOSA (personal communication, April 14, 2025). Additionally, "Doing everything at the same time regulation, implementation, use cases caused delays" (personal communication, April 14, 2025). This sentiment is echoed by private sector representatives who criticized the Commission's broad focus. "They did not have a clear priority. That broad focus took away direction from development teams" (personal communication, April 29, 2025)

Fourth, reusability and interoperability are crucial. An expert from the private sector highlights the importance of leveraging existing systems. "Try to reuse what was already there such as identity cards, existing eID apps, qualified signatures. That was kind of missing," (personal communication, April 29, 2025). Failure to reuse infrastructure risks wasting public resources and creating redundant systems. Interoperability is especially important in the EU context, where Member States have diverse identity systems. "France does not even have a National Register like we do. The lesson is not to copy each other, but to ensure interoperability," emphasized an expert (personal communication, April 14, 2025).

Finally, the importance of trust and public-private collaboration was highlighted repeatedly. FPS Economy stressed the need to tap into external expertise. "There is a lot

of knowledge outside the public system… but the more parties involved, the harder it is to find balance" (personal communication, April 30, 2025). Building public trust will also be essential for adoption. "We will need a lot of trust-building, skill development, and communication… or citizens will not use the wallet" (personal communication, April 30, 2025).

6 Discussion

This discussion section synthesizes the comparative findings on the EUDIW implementation in Estonia and Belgium to address the central research question, namely "What are the key factors shaping the implementation strategies of the European Digital Identity Wallet (EUDIW) in Estonia and Belgium, and how can these insights inform a cohesive EU-wide approach?". To do so, the chapter synthesizes the findings of the three-sub research questions presented in the previous chapter. That are:

1. Who are the key stakeholders in Estonia and Belgium involved in the adoption and implementation of the EUDIW, and what are their roles, interests, and objectives?

2. What are the drivers and barriers for stakeholders in EUDIW implementation?

3. How do Estonia's and Belgium's EUDIW implementation strategies differ, and what lessons can they offer for the broader EU rollout?

Previous studies have shown that the success of digital identity initiatives depends not only on technical infrastructure but also on the alignment of actors, institutions, and policy environments (Degen & Teubner, 2024; Elbanna, 2012; Kostic, 2024; Lukkien et al., 2023; Pouloudi et al., 2004). This discussion builds on such insights by comparing the implementation strategies of two EU Member States through the lenses of ANT and PESTEL.

Drawing from Actor-Network Theory (ANT) and PESTEL analysis while also drawing connection to the academic literature that is introduced in the second chapter of this study, the section integrates stakeholder dynamics, drivers and barriers, and national implementation strategies to examine what these divergent cases reveal about the feasibility and fragility of a harmonized European digital identity wallet implementation.

6.1 Stakeholder Ecosystems and Network Building

In both Estonia and Belgium, the EUDIW implementation process is shaped by complex and evolving stakeholder networks. Using ANT as a lens, these networks can be understood as socio-technical systems constructed through actor alignments. As Elbanna (2012) emphasizes, power in such systems is not possessed but performed through network alliances. This was evident in Belgium, where such as the separation between BOSA, FPS Interior, FPS Economy, and CCB created distributed responsibility, while in Estonia, RIA consolidated influence among internal departments.

A central tenet of ANT is that network building occurs through translation a process in which a network initiator defines roles, recruits actors, and ensures their alignment through problematization, interessement, enrollment, and mobilization (Callon, 1984). In Estonia, the Information System Authority (RIA) has clearly emerged as the main network builder. It has set itself up as the obligatory passage point by taking responsibility for procurement, coordination, and integration of the wallet infrastructure. Problematization is visible in RIA's efforts to implement the EUDIW as a necessary evolution of Estonia's existing eID ecosystem. Interessement is pursued through open-market procurement and structured collaboration with private actors. Enrollment happens as RIA works to define the wallet's technical and legal architecture while keeping supervisory roles within the same institution a structure that, while practical and facilitating efficient coordination across domains like architecture, security, and infrastructure, creates concern since supervisory authorities cannot contradict with other roles even though the responsibilities are undertaken by different departments it is still the same organization.

In Belgium, network translation is more fragmented. The implementation is led through distributed translation efforts involving BOSA, FPS Interior, CCB, and FPS Economy. Each actor defines its own problematization and interests. BOSA emphasizes authentication and technical deployment, while FPS Interior controls access to authentic sources like the National Register. CCB oversees cybersecurity and certification, and FPS Economy is responsible for trust services. As one CCB representative noted, "We report to different ministers, which helps preserve independence but can hinder swift decision-making" (personal communication, April 30, 2025). Additionally, Belgium's federal system introduces horizontal fragmentation, particularly between federal and regional authorities. Enrollment was stalled due to political uncertainty and diverging timelines, especially in coordinating with regional actors or agreeing on supervisory arrangements.

ANT highlights that power is not a possession, but the outcome of a successfully aligned and stabilized network (Elbanna, 2012). This study finds that non-human actors such as the eIDAS regulation, EU implementing acts, certification schemes, and technical standards are central to this performance of power. They do not only enable action, but they constrain it. For instance, the absence of a finalized EU-wide certification scheme has stalled progress even in technically advanced eID ecosystem like Estonia. Similarly, in Belgium, the uncertainty around legal definitions and trust service obligations under eIDAS 2.0 has led to reliance on ad hoc workarounds. In both cases, non-human actors such as certification schemes, EU regulations and requirements shape not just what is possible, but also who can act, when, and with what degree of legitimacy.

This insight aligns with Elbanna's (2012) emphasis on how artefacts, organizations, and regulations co-constitute actor-networks. In practical terms, it reveals how implementation struggles are not simply about misaligned stakeholder interests, but about unstable or incomplete alignment of sociotechnical elements needed to perform and sustain power.

ANT also encourages a symmetrical view of global and local dynamics. It does not privilege one level over the other but sees them as co-constructed through actor-networks (Elbanna, 2012). Estonia's EUDIW implementation strategy exemplifies this symmetry. It reflects a global push for interoperability and alignment with EU objectives while adapting to local capacities and institutional history. Estonia's strategy of outsourcing wallet development to private vendors, rather than building in-house, reflects not only resource pragmatism but also a locally informed approach to global mandates. On the other hand, in Belgium, the global-local interaction is more strained. Regional governance complexities and evolving national politics mean that translating EU-level priorities into national action often results in friction. For example, Belgium's decision to advance with wallet prototyping before legal certainty was achieved reflects pressure from EU timelines but also reveals local tensions in how policy goals are interpreted and prioritized.

6.2 Drivers and Barriers

By integrating PESTEL with ANT, this study acknowledges that actor-networks are not built in a vacuum. They are embedded within broader political, economic, social, technological, environmental, and legal environments that shape the conditions under which translation and power performance occur. Across both countries, PESTEL analysis revealed overlapping as well as divergent drivers and barriers that influence stakeholder motivation and capacity to engage. The findings from expert interviews showed that drivers and barriers are in line with the findings of earlier research on the wallet in the academic literature as discussed in the literature review section of this research (Degen & Teubner, 2024; Khayretdinova et al., 2022; Kostic, 2024; Lukkien et al., 2023).

6.2.1 Political Drivers and Barriers

In both contexts, sovereignty and data autonomy were cited as primary drivers, particularly in response to fears of platform dominance by American tech giants. As Belgian stakeholders emphasized, "We do not want Apple's mobile ID to dominate" (personal communication, April 14, 2025). Similarly, experts from Estonia framed the EUDIW as a geopolitical tool to reinforce European autonomy (personal communication, April 21, 2025).

Yet, political uncertainty hindered progress in both settings. Belgium faced a prolonged period without a government that delayed decisions. In Estonia, ambiguity of role distribution among involved institutions creates confusion within the ecosystem. Stakeholders in both countries expressed frustration at the rushed legislative timelines imposed by the EU, which left national actors with vague technical targets and political pressure to comply.

In Belgium, the distribution of responsibilities across regional and federal levels has further complicated implementation. “There are diverging opinions… not always at the same level or with the same political objectives,” noted one official (personal communication, April 14, 2025), especially in domains like diplomas and driving licenses, which fall under regional competencies.

Estonia’s implementation is also shaped by intra-institutional overlap. RIA’s dual role as wallet implementer and as the supervisory body raises concerns about the separation of powers. As noted by one stakeholder, “We are procuring the wallet, but the supervisory authority is in the same organization. That’s not ideal” (personal communication, April 11, 2025).

6.2.2 Economic Drivers and Barriers

In Estonia, economic pragmatism drives reliance on public-private partnerships for wallet provisioning and attestation infrastructure. As an expert noted, “We will not build the wallet ourselves we will procure it from the private sector” (personal communication, April 25, 2025). Estonia’s procurement-based strategy reflects also an effort to mobilize private-sector actors into a national implementation network, in line with ANT’s view of stakeholder enrolment as a mechanism of network building.

Belgium also aims for budgetary efficiency by consolidating existing authentication tools into one wallet. However, both countries reported resource constraints, especially the high cost of dual ecosystems and uncertainty around funding for scaling up. As one Belgian official put it, “We developed something we may have to throw away in two years because the standards changed” (personal communication, April 14, 2025).

6.2.3 Social Drivers and Barriers

In Estonia, widespread digital literacy and a strong e-government legacy increase social readiness. However, even there, officials admitted struggling to justify the need for a wallet in a country that already has functioning eID systems.

In Belgium, officials see the wallet as a solution to accessibility problems such as removing the need for card readers. However, public confusion remains high. Misunderstandings about its relationship to existing apps like itsme and a lack of communication have hindered buy-in. As one stakeholder explained, “Ministers thought it was just a competitor to itsme” (personal communication, April 14, 2025).

In both countries, the need for a “killer application” was seen as crucial to generate user adoption. Belgian respondents highlighted mobile driving licenses and pseudonymized attestations such as age verification as use cases that could provide everyday value and drive uptake. “The killer attestation is what would show people the utility of the wallet,” explained one stakeholder (personal communication, April 14, 2025).

Public trust and understanding remain underdeveloped. In Belgium, stakeholders emphasized the need for extensive communication campaigns, not only for the public but also internally within government. “We spend 70% of our time explaining what the wallet is and what it is not,” one official said (personal communication, April 14, 2025).

6.2.4 Technological Drivers and Barriers

In Belgium, previous investments in pandemic-related infrastructure proved useful. “We reused the experience from building the COVID certificate app” explained one official (personal communication, April 30, 2025), allowing them to fast-track digital attestations within MyGov.be. Similarly, Estonia is capitalizing on its existing national architecture. As one interviewee noted, “We are using components like the eIDAS node and X-Road to keep integration efficient” (personal communication, April 11, 2025).

Belgium and Estonia both emphasized device-level security risks, especially the inability to control operating systems like iOS and Android. Belgium has opted for a phased rollout, while Estonia is prioritizing procurement and integration based on existing components like X-Road and eIDAS nodes. Both countries highlighted lack of reference implementations from the EU as a major barrier, leaving them to work “ad hoc” in Belgium or to “build parallel systems” in Estonia without assurance of long-term interoperability (personal communication, April 14, 2025; personal communication, April 25, 2025).

Both countries flagged a wider issue with the European digital ecosystem. EU-wide technical guidance lags behind political ambition. “We need clearer specs, not just political will,” noted one Estonian expert (personal communication, April 25, 2025).

6.2.5 Environmental Drivers and Barriers

One of the most striking cross-cutting observations from both country cases is the complete absence of environmental considerations in stakeholder narratives surrounding the implementation of the European Digital Identity Wallet. None of the Estonian or Belgian interviewees referenced sustainability, energy use, environmental procurement standards, or digital carbon footprints in their discussions of wallet-related infrastructure, design, or deployment.

There are several possible explanations for this omission. First, the dominant political and legal framing of the EUDIW, particularly the urgency to comply with eIDAS 2.0 within strict timelines may be crowding out broader or longer-term considerations such as sustainability. Second, institutional compartmentalization where environmental and digital policymaking are handled by separate ministries or units may mean that environmental impact assessments or green standards are not integrated into digital infrastructure planning by default.

The absence of environmental discourse should not be interpreted as evidence that environmental impacts are negligible. As digital infrastructures expand, they inevitably contribute to energy consumption and resource use. Moreover, as the European Green Deal and related strategies increasingly link digital transformation to sustainability goals, the lack of environmental awareness in national digital identity planning could emerge as a blind spot in both governance and implementation.

This analytical gap suggests a need for further research and potentially policy intervention to embed environmental considerations into digital identity development. Future phases of EUDIW deployment such as procurement, lifecycle management, or cross-border data flows present opportunities to introduce sustainability criteria. Doing so could align digital infrastructure planning more closely with the EU's twin digital and green transitions.

6.2.6 Legal Drivers and Barriers

eIDAS 2.0 serves as the primary legal driver, providing legitimacy for implementation and justifying investment. However, both Estonia and Belgium flagged the piecemeal nature of implementing acts as disruptive. In Estonia, regulatory uncertainty interfered with procurement timelines. On the other hand, in Belgium, changing requirements undermined early development.

Moreover, both countries pointed to certification gaps as a significant risk. As an expert from Estonia highlighted the absence of national expertise to design or manage

certification schemes “We still lack national capacity to run certification schemes” (personal communication, April 25, 2025). While Belgium warned that fragmented certification across Member States could erode cross-border trust (personal communication, April 30, 2025).

The absence of finalized supervisory frameworks has led to a cautious implementation style. As one Belgian expert stated, “We cannot certify private wallets until we know who supervises them and under what standards” (personal communication, April 30, 2025).

6.3 Implementation Strategies and Lessons Learned

The implementation of the European Digital Identity Wallet in Estonia and Belgium reveals two distinct strategic approaches shaped by national governance models, technical maturity, and stakeholder dynamics. The exploration of these cases provide insight into how national strategies adapt to the challenges of European-level coordination and what broader lessons can be drawn for an EU-wide rollout.

Estonia has adopted a modular and market-based strategy centered on procurement. The Information System Authority (RIA) coordinates the effort, relying heavily on the private sector to deliver wallet services while retaining control over integration and interoperability. This approach capitalizes on Estonia’s advanced digital infrastructure, including systems like X-Road and the eIDAS node, and reflects the country’s longstanding emphasis on public-private collaboration. As one official explained, “We are not going to build the wallet ourselves. We are going to procure it as a service” (personal communication, April 25, 2025).

In contrast, Belgium has opted for a phased, state-led rollout built around the MyGov.be application. The strategy is defined by a strict separation of roles and responsibilities. BOSA develops the application, the CCB manages cybersecurity and certification, and FPS Economy oversees trust services. This clear division supports transparency and accountability but often complicates cross-agency coordination, especially under conditions of political uncertainty or shifting ministerial priorities. As one stakeholder put it, “We were without a government for eight months… which does not help to get a clear position from the political level” (personal communication, April 8, 2025).

From these cases, several key lessons emerge that are relevant across the EU. First, both Estonia and Belgium encountered major challenges due to the lack of stable EU-level technical guidance during the initial rollout. Belgian stakeholders described the situation as “Doing everything at the same time without knowing what would be reusable leading to duplication and wasted resources” (personal communication, April 14, 2025). In

Estonia, the lack of finalized standards has delayed procurement and led to uncertainty around certification and liability structures.

Second, the timing and sequencing of development matter. Belgium's phased strategy, while slower, allows for better alignment with evolving EU requirements. However, without the finalized guidelines the risk of redundancy remains.

Third, institutional capacity and coordination are critical. Belgium's compartmentalized model ensures clear mandates but suffers from fragmentation, while Estonia's concentrated authority within RIA facilitates agility but introduces potential conflicts of interest since the responsible authority is the same institution even though the roles are given to different departments. This reflects Actor-Network Theory's proposition that network-building requires effective translation and alignment across multiple domains.

Fourth, both cases highlight the risks of over-reliance on a small group of experts. As one Estonian stakeholder noted, "The same five experts are in every working group, creating bottlenecks in decision-making and risking burnout" (personal communication, April 11, 2025). Broader engagement with industry and civil society will be necessary to scale the EUDIW ecosystem sustainably.

Finally, clear use cases and user value must be prioritized. As one Estonian respondent argued, "We still do not have a killer app that explains why people need another ID app" (personal communication, April 11, 2025). Belgium faces similar challenges, with some stakeholders fearing the wallet is misunderstood as a competitor to existing apps like itsme (personal communication, April 14, 2025).

Together, these lessons emphasize that successful EUDIW implementation depends not only on technical execution but on adaptive governance, collaborative alignment, and ongoing EU guidance. The Belgian and Estonian cases demonstrate that while national conditions differ, shared challenges require coordinated solutions at both the European and domestic levels.

7 Conclusion

7.1 Summary

This research investigated the factors shaping the national implementation strategies of the European Digital Identity Wallet (EUDIW) in Estonia and Belgium, with a focus on stakeholder roles, interests, and the broader political, economic, social, technological, environmental, and legal environments in which these strategies unfold. The study drew on Actor-Network Theory (ANT) and PESTEL analysis to analyze the socio-technical systems underlying implementation processes. It found that the development and rollout of EUDIW are shaped by complex and evolving ecosystems, where both human and non-human actors (such as legal regulations, technical standards, and digital infrastructures) exert power through dynamic network alignments. Although both countries are early movers, Estonia's approach is characterized by centralized coordination led by the Information System Authority (RIA), while Belgium's implementation reflects a more fragmented, federated model with distributed responsibilities among federal institutions and emerging regional actors.

The first sub-research question aimed to identify and analyze the primary stakeholders involved in the adoption and implementation of the EUDIW in Estonia and Belgium. It further sought to explore their roles, interests, and objectives. While the European Commission's Common Union Toolbox outlines the ideal ecosystem of stakeholders, this research used expert interviews and Actor-Network Theory (ANT) to provide an overview of these roles within the specific sociotechnical ecosystems of Estonia and Belgium, including the role of non-human actors such as regulations, technical standards, and infrastructure components. In Estonia, the process is largely coordinated by RIA, with support from the Ministry of Justice and the Ministry of the Interior. RIA not only leads procurement and integration but also performs regulatory interpretation, acting as a central network builder. In Belgium, the Federal Public Service for Policy and Support (BOSA) plays a key implementation role, working alongside institutions such as FPS Interior, CCB, and FPS Economy. However, power is more dispersed, reflecting Belgium's layered federal structure. ANT revealed that both countries face challenges related to aligning these actors, especially in translating EU-level goals into coherent national strategies.

The second sub-research question By integrating PESTEL analysis with ANT, this study acknowledges that actor-networks do not form in isolation but are shaped by the broader political, economic, social, technological, environmental, and legal landscape. The PESTEL framework revealed that while political drivers such as digital sovereignty and

EU compliance incentivize action, challenges like political fragmentation in Belgium and institutional role ambiguity in Estonia hinder progress. Economically, both countries struggle with resource constraints and uncertainty regarding future technical standards. Additionally, in both countries representatives of the private sector raise strong skepticism regarding the added market value of the wallet. Social readiness varies between two countries. Estonia benefits from digital literacy and trust in government systems even though the added value of the new wallet solution remains as a question. On the other hand, Belgium faces public confusion about what the wallet is and how does it differ from the existing authentication app itsme and show skepticism. Technologically, both countries are building on existing infrastructures but face significant barriers due to a lack of standardized EU guidance and incomplete certification schemes. Crucially, environmental considerations are absent from both national strategies. Legally, uncertainty around supervisory structures and certification requirements continues to delay implementation.

The third sub-research question explored how Estonia's and Belgium's EUDIW implementation strategies differ and what lessons they offer for the EU-wide rollout. The findings reveal two distinct approaches shaped by national governance models, technical readiness, and coordination structures. Estonia follows a centralized, procurement-based model led by the Information System Authority (RIA), leveraging a mature digital infrastructure and strong public-private collaboration. In contrast, Belgium adopts a phased, state-led rollout centered on the MyGov.be app, with responsibilities distributed across institutions like BOSA, FPS Interior, and CCB. This structure enables transparency but complicates cross-agency coordination, especially during political uncertainty. Importantly, both countries struggle with public-facing adoption due to unclear user value. Without compelling use cases, there is a risk the wallet will be seen as redundant. This suggests that alongside technical and institutional readiness, user-centric design and clear communication are essential for successful rollout.

These insights inform the main research question "What are the key factors shaping the implementation strategies of the European Digital Identity Wallet in Estonia and Belgium, and how can these inform a cohesive EU-wide approach?". The findings show that national strategies are shaped by actor-networks comprising institutional mandates, political dynamics, and technical infrastructures and are further influenced by external PESTEL factors such as legal ambiguity, economic uncertainty, and social readiness. Both Estonia and Belgium highlight the need for stable EU-level coordination, adaptive national governance, and cross-sector alignment. These lessons underscore that while national conditions vary, common implementation challenges demand flexible but harmonized EU support mechanisms.

By answering the three sub-questions and synthesizing their insights, this research contributes to a deeper understanding of EUDIW implementation at the Member State level filling a critical gap in current literature that has focused predominantly on the technological design of the wallet. The comparative cases of Estonia and Belgium provide empirically grounded guidance for other Member States navigating the complex path toward digital identity integration.

7.2 Limitations and Future Research

This study offers important insights into national EUDIW implementation strategies, but it is subject to several limitations that also offer room for future research. The primary limitation lies in the evolving nature of the EUDIW ecosystem. As expert interviews and prior literature indicate, both EU-level and national implementation processes are still in flux. Key elements such as implementing acts, technical standards, and certification schemes, especially those to be finalized by the European Commission and ENISA, remain incomplete. At the national level, corresponding certification frameworks are also lacking. Consequently, stakeholder roles and strategies are still forming, making it difficult to capture a fully stabilized picture. Future research will benefit from re-examining national strategies once more regulatory clarity and implementation progress are achieved.

Second, no EUDI Wallet has yet been officially launched in any Member State under the finalized EU criteria, although national applications like MyGov.be are being adapted toward this goal. As a result, this study could not assess end-user adoption. Future research should investigate citizens' and businesses' willingness to adopt the wallet once compliant versions are deployed. As experts noted, while providing the wallet will be mandatory for Member States, its success ultimately depends on its uptake by users in daily use.

In a similar vein, the wallet's contribution to strengthening the European Single Market and digital sovereignty will depend heavily on engagement from the private sector. Future studies should explore how industry actors, including SMEs, perceive the wallet and what incentives or barriers shape their integration efforts.

Finally, although the PESTEL framework highlighted a broad range of external influences, one notable gap concerning environmental factors emerged. None of the Estonian or Belgian experts mentioned sustainability, energy use, or digital carbon footprints. This gap should not be interpreted as a sign of negligible impact but rather as a missing dimension in current policy discourse. Future research is needed to uncover

why environmental aspects are excluded and how they might be meaningfully integrated into digital identity strategies going forward.

Declaration of Authorship

I hereby declare that, to the best of my knowledge and belief, this Master Thesis titled "The Road to EU-Wide Digital Identity Wallet Adoption: Insights from Estonia and Belgium's EUDI Wallet Implementation" 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.

Brussels, 08 September 2025

Alper Tanrıverdi

Consent Form

for the use of plagiarism detection software to check my thesis

Name: Tanrıverdi
Given Name: Alper
Student number: r0966215
Course of Study: Public Sector Innovation and eGovernance
Address: Rue François Bossaerts 49, 1030 Brussels
Title of the thesis: The Road to EU-Wide Digital Identity Wallet Adoption: Insights from Estonia and Belgium's EUDI Wallet Implementation

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.

Rue François Bossaerts 49, 1030 Brussels

Brussels, 02 June 2025

Alper Tanrıverdi

References

Abraham, A., Schinnerl, C., & More, S. (2021). SSI Strong Authentication using a Mobile-phone based Identity Wallet Reaching a High Level of Assurance: *Proceedings of the 18th International Conference on Security and Cryptography*, 137–148. https://doi.org/10.5220/0010542801370148

Bejussova, K., Lips, S., Ahmed, R. K., & Draheim, D. (2024). Assessment of the eID Ecosystem as a Part of the State's Critical Infrastructure: The Case of Estonia. In A. Kö, G. Kotsis, A. M. Tjoa, & I. Khalil (Eds.), *Electronic Government and the Information Systems Perspective* (Vol. 14913, pp. 88–102). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-68211-7_8

Biernacki, P., & Waldorf, D. (1981). Snowball Sampling: Problems and Techniques of Chain Referral Sampling. *Sociological Methods & Research*, *10*(2), 141–163. https://doi.org/10.1177/004912418101000205

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Brans, M., De Visscher, C., & Vancoppenolle, D. (2006). Administrative reform in Belgium: Maintenance or modernisation? *West European Politics*, *29*(5), 979–998. https://doi.org/10.1080/01402380600968869

Cadle, J., Paul, D., & Turner, P. (2010). *Business analysis techniques: 72 essential tools for success*. British Computer Society.

Callon, M. (1984). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. *The Sociological Review*, *32*(1_suppl), 196–233. https://doi.org/10.1111/j.1467-954X.1984.tb00113.x

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? Research

case examples. *Journal of Research in Nursing*, *25*(8), 652–661. https://doi.org/10.1177/1744987120927206

Carr, D. (2021). Personal identity is social identity. *Phenomenology and the Cognitive Sciences*, *20*(2), 341–351. https://doi.org/10.1007/s11097-020-09702-1

Clarke, V., & Braun, V. (2017). Thematic analysis. *The Journal of Positive Psychology*, *12*(3), 297–298. https://doi.org/10.1080/17439760.2016.1262613

Cordella, A., Paletti, A., & Shaikh, M. (2018). *Renegotiating Public Value with Co-Production* (Vol. 1). Oxford University Press. https://doi.org/10.1093/oso/9780198816225.003.0008

Corici, A. A., Podgorelec, B., Zefferer, T., Hühnlein, D., Cucurull, J., Graux, H., Dedovic, S., Romanov, B., Schmidt, C., & Krimmer, R. (2022). Enhancing European Interoperability Frameworks to Leverage Mobile Cross-Border Services in Europe. *DG.O 2022: The 23rd Annual International Conference on Digital Government Research*, 41–53. https://doi.org/10.1145/3543434.3543638

Cybernetica. (2024, June 21). *Estonian digital identity wallet MVP*. https://cyber.ee/resources/news/estonian-digital-identity-wallet-mvp/

Czerny, R., Kollmann, C., Podgorelec, B., Prünster, B., & Zefferer, T. (2023). Smoothing the Ride: Providing a Seamless Upgrade Path from Established Cross-Border eID Workflows Towards eID Wallet Systems: *Proceedings of the 20th International Conference on Security and Cryptography*, 460–468. https://doi.org/10.5220/0012091900003555

DC4EU. (2025, March 17). *Digital Credentials for Europe*. DC4EU. https://www.dc4eu.eu/

De Cock, D., Wolf, C., & Preneel, B. (2006). *The Belgian Electronic Identity Card (Overview)*. 298–301.

https://www.researchgate.net/publication/221307194_The_Belgian_Electronic_Identity_Card_Overview

De Jong, M. D. T., Neulen, S., & Jansma, S. R. (2019). Citizens' intentions to participate in governmental co-creation initiatives: Comparing three co-creation configurations. *Government Information Quarterly*, *36*(3), 490–500. https://doi.org/10.1016/j.giq.2019.04.003

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

Döringer, S. (2021). 'The problem-centred expert interview'. Combining qualitative interviewing approaches for investigating implicit expert knowledge. *International Journal of Social Research Methodology*, *24*(3), 265–278. https://doi.org/10.1080/13645579.2020.1766777

Dumortier, J., & Robben, F. (2010). User and Access Management in Belgian e-Government. In N. Pohlmann, H. Reimer, & W. Schneider (Eds.), *ISSE 2009 Securing Electronic Business Processes* (pp. 97–107). Vieweg+Teubner. https://doi.org/10.1007/978-3-8348-9363-5_9

Dunleavy, P. (2005). New Public Management Is Dead—Long Live Digital-Era Governance. *Journal of Public Administration Research and Theory*, *16*(3), 467–494. https://doi.org/10.1093/jopart/mui057

e-Estonia. (2024, February 14). *Digital wallet and eIDAS 2.0: A boost for Estonian companies*. e-Estonia. https://e-estonia.com/digital-wallet-and-eidas-2-0-a-boost-for-estonian-companies/

Elbanna, A. (2012). Applying Actor Network Theory and Managing Controversy. In *Information systems theory: Explaining and predicting our digital society* (pp. 117–130). Springer.

ENISA. (2024, April 18). *The European Digital Identity Wallet: An EU Challenge*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.enisa.europa.eu/sites/default/files/all_files/The%20EUDI%20Wallet_An%20EU%20challenge.pdf

EUR-Lex. (2021). *COM/2021/281*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0281

European Commission. (2023a, February 10). *European Digital Identity Wallets: Commission publishes first technical Toolbox towards prototypes*. https://digital-strategy.ec.europa.eu/en/news/european-digital-identity-wallets-commission-publishes-first-technical-toolbox-towards-prototypes

European Commission. (2023b, February 10). *The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework*. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

European Commission. (2024, December 4). *Commission adopts technical standards for cross-border European Digital Identity Wallets*. https://digital-strategy.ec.europa.eu/en/news/commission-adopts-technical-standards-cross-border-european-digital-identity-wallets

European Commission. (2025, February 21). *European Digital Identity (EUDI) Regulation*. https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation

European Digital Identity Wallet. (2025). *The Technical Specifications Behind EU Digital Identity Wallets*. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Technical+Specifications

European Parliament. (2022, March 7). *Revision of the eIDAS Regulation: Findings on its implementation and application*.

https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)699491

Eurostat. (2024). *E-government activities of individuals via websites* [Dataset]. Eurostat. https://doi.org/10.2908/ISOC_CIEGI_AC

EWC. (2023, May 2). *About Us—EUDI Wallet Consortium*. https://eudiwalletconsortium.org/about-us/

Fairchild, A., & de Vuyst, B. (2012). *The Evolution of the e-ID card in Belgium: Data Privacy and Multi Application Usage*. Sixth International Conference on Digital Society.

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods*, *5*(1), 80–92. https://doi.org/10.1177/160940690600500107

Fridell, T., Vangen, G., Mincer-Daszkiewicz, J., Norder, J.-J., Drvodelić, I., Rautio, K., & Bacharach, G. (2023). *The future is in your wallet – how EMREX plans interaction with the EUDI wallet*. *95*, 209–2015.

Giddens, A. (1991). Modernity and self-identity: Self and society in the late modern age Introduction. In *Modernity and self-identity: Self and society in the late modern age* (Reprint). Polity Press.

Gläser, J., & Laudel, G. (2009). On Interviewing "Good" and "Bad" Experts. In *Interviewing Experts* (pp. 117–137). Palgrave Macmillan UK. https://doi.org/10.1057/9780230244276_6

Gur, F. A., & Mathias, B. D. (2021). Finding Self Among Others: Navigating the Tensions Between Personal and Social Identity. *Entrepreneurship Theory and Practice*, *45*(6), 1463–1495. https://doi.org/10.1177/10422587211038109

Harbach, M., Fahl, S., Rieger, M., & Smith, M. (2013). On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards. In E. De Cristofaro & M. Wright (Eds.), *Privacy Enhancing Technologies* (Vol. 7981, pp. 245–264). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39077-7_13

Information System Authority, R. of E. (2024, January 21). *Digital wallet, or the European Union Digital Identity application (EUDI Wallet)*. https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/eudi-wallet

Jack, E. P., & Raturi, A. S. (2006). Lessons learned from methodological triangulation in management research. *Emerald Group Publishing Limited*, *29*, 345–357. https://doi.org/10.1108/01409170610683833

Jøsang, A., & Pope, S. (2005). *User centric identity management*. 77–89.

Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Khayretdinova, A., Kubach, M., Sellung, R., & Roßnagel, H. (2022). Conducting a Usability Evaluation of Decentralized Identity Management Solutions. In M. Friedewald, M. Kreutzer, & M. Hansen (Eds.), *Selbstbestimmung, Privatheit und Datenschutz* (pp. 389–406). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-33306-5_19

Kitchenham, B., Pretorius, R., Budgen, D., Pearl Brereton, O., Turner, M., Niazi, M., & Linkman, S. (2010). Systematic literature reviews in software engineering – A tertiary study. *Information and Software Technology*, *52*(8), 792–805. https://doi.org/10.1016/j.infsof.2010.03.006

Korir, M., Parkin, S., & Dunphy, P. (2022). An Empirical Study of a Decentralized IdentityWallet Usability, Security, and Perspectives on User Control. *Proceedings of the 18th Symposium on Usable Privacy and Security, SOUPS 2022*, 195–211. https://www.usenix.org/conference/soups2022/presentation/korir

Kostic, S. (2024). Who is the Better Operator of an Identity Wallet Prioritised by the User? - A Quantitative Survey Between State and Company. *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 1–7. https://doi.org/10.1145/3613905.3647961

Landrigan, M., Wilson, S., & Fraser, H. (2023). Why Are There So Many Digital Identities? *Law, Technology and Humans*. https://doi.org/10.5204/lthj.3096

Latour, B. (1996). On actor-network theory: A few clarifications. *Soziale Welt*, *47(4)*, 369–381.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice*, *5*(4), 379–393. https://doi.org/10.1007/BF01059830

Lips, S., Aas, K., Pappel, I., & Draheim, D. (2019). Designing an Effective Long-Term Identity Management Strategy for a Mature e-State. In A. Kő, E. Francesconi, G. Anderst-Kotsis, A. M. Tjoa, & I. Khalil (Eds.), *Electronic Government and the Information Systems Perspective* (Vol. 11709, pp. 221–234). Springer International Publishing. https://doi.org/10.1007/978-3-030-27523-5_16

Lips, S., Tsap, V., Bharosa, N., Krimmer, R., Tammet, T., & Draheim, D. (2023). Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership: Learning from the Case of Estonia. *Information Systems Frontiers*, *25*(6), 2439–2456. https://doi.org/10.1007/s10796-022-10363-5

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

Mackieson, P., Shlonsky, A., & Connolly, M. (2019). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis. *Qualitative Social Work*, *18*(6), 965–980. https://doi.org/10.1177/1473325018786996

Mander, S., Lips, S., & Draheim, D. (2023). The Utilization of Public-Private Partnership Frameworks in the Management of eID Projects. In A. Kö, E. Francesconi, A. Asemi, G. Kotsis, A. M. Tjoa, & I. Khalil (Eds.), *Electronic Government and the Information Systems Perspective* (Vol. 14149, pp. 17–32). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-39841-4_2

Manzi, C., & Benet-Martinez, V. (2022). Multiple identities juggling game: Types of identity integration and their outcomes. *Self and Identity*, *21*(5), 501–505. https://doi.org/10.1080/15298868.2022.2067222

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

Meuser, M., & Nagel, U. (2009). The Expert Interview and Changes in Knowledge Production. In *Interviewing Experts* (pp. 17–42). Palgrave Macmillan UK. https://doi.org/10.1057/9780230244276_2

Miles, S. (2017). Stakeholder Theory Classification: A Theoretical and Empirical Evaluation of Definitions. *Journal of Business Ethics*, *142*(3), 437–459. https://doi.org/10.1007/s10551-015-2741-y

Morgan, D., & Parsovs, A. (2017). Using the Estonian Electronic Identity Card for Authentication to a Machine. In H. Lipmaa, A. Mitrokotsa, & R. Matulevičius (Eds.), *Secure IT Systems* (Vol. 10674, pp. 175–191). Springer International Publishing. https://doi.org/10.1007/978-3-319-70290-2_11

Morgan, H. (2022). Conducting a Qualitative Document Analysis. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2022.5044

MyGov.be. (2024). *Direct Access to Your Digital Public Services*. https://mygov.be/

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. *International Journal of Qualitative Methods*, *22*, 16094069231205789. https://doi.org/10.1177/16094069231205789

NOBID Consortium. (2022). *About NOBID Consortium*. NOBID Consortium. https://www.nobidconsortium.com/about/

Nurmi, J., & Niemelä, M. S. (2018). PESTEL Analysis of Hacktivism Campaign Motivations. In N. Gruschka (Ed.), *Secure IT Systems* (Vol. 11252, pp. 323–335). Springer International Publishing. https://doi.org/10.1007/978-3-030-03638-6_20

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

Pöhn, D., & Hommel, W. (2020). An overview of limitations and approaches in identity management. *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 1–10. https://doi.org/10.1145/3407023.3407026

Potential. (2023). Our ambitions. *Potential - For European Digital Identity*. https://www.digital-identity-wallet.eu/our-ambitions/

Pouloudi, A., Gandecha, R., Atkinson, C., & Papazafeiropoulou, A. (2004). How Stakeholder Analysis Can Be Mobilized With Actor-network Theory To Identify Actors. *Information Systems Research: Relevant Theory And Informed Practice*, 705–711.

Preukschat, A., & Reed, D. (2021). *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Manning.

Prusa, J. (2015). *E-identity: Basic Building Block of e-Government*.

Regulation (EU) 910/2014, 257 OJ L (2014). http://data.europa.eu/eli/reg/2014/910/oj/eng

Regulation (EU) 2024/1183 (2024). http://data.europa.eu/eli/reg/2024/1183/oj/eng

Ricci, S., Janout, V., Parker, S., Jerabek, J., Hajny, J., Chatzopoulou, A., & Badonnel, R. (2021). PESTLE Analysis of Cybersecurity Education. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–8. https://doi.org/10.1145/3465481.3469184

Scupola, A., & Mergel, I. (2022). Co-production in digital transformation of public administration and public value creation: The case of Denmark. *Government Information Quarterly*, *39*(1), 101650. https://doi.org/10.1016/j.giq.2021.101650

Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, *40*(1), 101781. https://doi.org/10.1016/j.giq.2022.101781

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Somers, G., & Dumortier, J. (2006). A Trust Label for Secure and Compliant e-ID Applications: The Belgian Experience. In *ISSE 2006—Securing Electronic*

Busines Processes (pp. 356–362). Vieweg. https://doi.org/10.1007/978-3-8348-9195-2_38

Stewart, J. (2012). Multiple-case Study Methods in Governance-related Research. *Public Management Review*, *14*(1), 67–82. https://doi.org/10.1080/14719037.2011.589618

Swann, W. B., Gómez, Á., Seyle, D. C., Morales, J. F., & Huici, C. (2009). Identity fusion: The interplay of personal and social identities in extreme group behavior. *Journal of Personality and Social Psychology*, *96*(5), 995–1011. https://doi.org/10.1037/a0013668

Tan, E., & Crompvoets, J. (2022). Chapter 1: A new era of digital governance. In E. Tan & J. Crompvoets (Eds.), *The new digital era governance* (pp. 13–49). Brill | Wageningen Academic. https://doi.org/10.3920/978-90-8686-930-5_1

Van Roijen, D. (2024). The European Digital Identity Wallet: A Healthcare Perspective. *Blockchain in Healthcare Today*, *7*(2). https://doi.org/10.30953/bhty.v7.344

Walker, L. (2024, May 14). *Simplifying services: Belgium among first in EU to launch digital wallet*. The Brussles Times. https://www.brusselstimes.com/1045106/simplifying-services-belgium-among-first-in-eu-to-launch-digital-wallet-tbtb

Whittle, A., & Spicer, A. (2008). Is Actor Network Theory Critique? *Organization Studies*, *29*(4), 611–629. https://doi.org/10.1177/0170840607082223

Wohlin, C., Kalinowski, M., Romero Felizardo, K., & Mendes, E. (2022). Successful combination of database search and snowballing for identification of primary studies in systematic literature studies. *Information and Software Technology*, *147*, 106908. https://doi.org/10.1016/j.infsof.2022.106908

Zafeiropoulou, A., & Sakkopoulos, E. (2023). Harmonising Digital Identity Documents. *2023 14th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 1–8. https://doi.org/10.1109/IISA59645.2023.10345955

Zwattendorfer, B., Stranacher, K., & Zefferer, T. (2014). An Overview of Cloud Identity Management-Models: *Proceedings of the 10th International Conference on Web Information Systems and Technologies*, 82–92. https://doi.org/10.5220/0004946400820092