TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Inessa Victoria Mülts 232667IVGM

Shaping of The National Certification Framework for The European Digital Identity Wallet (EUDIW)

Master's thesis

Supervisor: Silvia Lips
PhD

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Inessa Victoria Mülts 232667IVGM

Euroopa Digitaalse Identiteedi Rahakoti (EUDIW) riikliku sertifitseerimisraamistiku kujundamine

Magistritöö

Juhendaja: Silvia Lips
PhD

Tallinn 2025

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Inessa Victoria Mülts

12.05.2025

Abstract

The revised eIDAS 2.0 Regulation introduces the European Digital Identity Wallet (EUDIW), which aims to provide EU citizens and businesses with a secure, interoperable and user-controlled tool for cross-border digital identity management. However, the lack of national certification frameworks poses a significant barrier to consistent implementation across member states. This thesis develops a conceptual framework to support the national certification of the European Digital Identity Wallet (EUDIW), with Estonia serving as a case study to examine institutional readiness and technical preparedness.

Drawing on expert interviews, legal and technical analysis and theoretical models from institutional governance, the study outlines key certification requirements, challenges and alignment strategies. It offers a conceptual framework and policy recommendations that can support member states in building robust, adaptable and trustworthy certification ecosystems for EUDIW. The findings contribute to EU-wide efforts to ensure secure digital identity services and reinforce user trust in cross-border interactions.

This thesis is written in English and is 74 pages long, including 9 chapters, 6 figures and 4 tables.

Keywords: EUDIW, framework, electronic identity, eIDAS, interoperability

Annotatsioon

Euroopa Digitaalse Identiteedi Rahakoti (EUDIW) riikliku sertifitseerimisraamistiku kujundamine

Euroopa Liidu eIDAS 2.0 määrus toob kasutusele Euroopa Digitaalse Identiteedi Rahakoti (EUDIW), mille eesmärk on pakkuda ELi kodanikele ja ettevõtetele turvalist, koostalitlusvõimelist ja kasutaja kontrollitavat digitaalse identiteedi haldustööriista piiriüleseks kasutamiseks. Käesolev magistritöö käsitleb EUDIW riikliku sertifitseerimisraamistiku kujundamise võimalusi, keskendudes eelkõige Eesti valmidusele ja institutsionaalsetele võimekustele.

Töös tuuakse välja põhilised nõuded, väljakutsed ja kooskõlastusvajadused sertifitseerimise valdkonnas, tuginedes ekspertintervjuudele ning tehnilis-õiguslikule ja teoreetilisele analüüsile. Lõputöö tulemusel pakutakse välja kontseptuaalne raamistik ning poliitikasoovitused, mis toetavad liikmesriike usaldusväärse ja kohanemisvõimelise sertifitseerimisraamistiku loomisel. Töö tulemused aitavad kaasa ELi eesmärgile tagada turvalised digitaalsed identiteediteenused ning suurendada kasutajate usaldust piiriülestes suhtluskeskkondades.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 74 leheküljel, 9 peatükki, 6 joonist, 4 tabelit.

Võtmesõnad: EUDIW, raamistik, elektrooniline identiteet, eIDAS, koostalitlusvõime

List of abbreviations and terms

AI	Artifical Intelligence
API	Application Programming Interface
ARF	Architecture and Reference Framework
CAB	Conformity Assessment Body
DID	Decentralized Identifier
EAA	Electronic Attestation of Attributes
EE	Estonia
eID	Electronic identification
eIDAS	Electronic Identification, Authentication and Trust Services
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUDI	European Union Digital Identity
EUDIW	European Union Digital Identity Wallet
GDPR	General Data Protection Regulation
JUSTDIGI	Ministry of Justice and Digital Affairs
MKM	Ministry of Economic Affairs and Communications
NFC	Near Field Communication
NOBID	The Nordic-Baltic eID
PID	Personal Identification Data
PKI	Public Key Infrastructure
PPA	The Estonian Police and Border Guard Board
QEAA	Qualified Electronic Attestation of Attributes
QTSP	Qualified Trust Service Provider
RIA	Estonian Information System Authority
SDG	Single Digital Gateway
TARA	Trusted Authentication and Recognition Architecture
TEE	Trusted Execution Environment
USA	United States of America

Table of contents

List of figures

List of tables

1 Introduction

In the rapidly evolving digital era, digital identity has emerged as a critical enabler for secure communication, trust and cross-border service provision in the European Union (EU). Recognizing the need for a harmonized legal and technical framework, the EU introduced the eIDAS Regulation in 2014, establishing a basis for the mutual recognition of electronic identification (eID) and trust services across member states (European Commission, 2014; Czerny et al., 2023). Since then, the EU's ambition for a digitally integrated market has intensified through initiatives such as the Digital Decade Policy Programme 2030, which sets forth strategic objectives for advancing Europe's digital sovereignty (European Parliament & Council of the European Union, 2022).

Despite this progress, new technological, societal and regulatory challenges have revealed the limitations of the original eIDAS framework. The increasing demand for mobile-first solutions, decentralized credentials and privacy-preserving technologies has accelerated the need for a more comprehensive, adaptable system (Sedlmeir et al., 2021). The first eIDAS Regulation, while pivotal, was not designed to fully address these emerging complexities (Hölbl et al., 2023).

In response to these developments, the European Commission introduced the revised eIDAS 2.0 Regulation (*Regulation (EU) 2024/1183*, 2024), placing the European Digital Identity Wallet (EUDIW) at the heart of the EU's digital identity ecosystem. The EUDIW is defined as a reliable, user-governed application allowing individuals and businesses to securely and seamlessly access wide range of public and private services across borders (European Commission, 2024f). According to Wimmer et al. (2018), the provision of integrated, interoperable digital services is fundamental to achieving the objectives of a connected Digital Single Market.

The deployment of the EUDIW, however, introduces new challenges that extend beyond traditional identity management. Certification of the Wallet, both from technical and regulatory standpoints, is vital for ensuring its trustworthiness, interoperability and security. Unlike earlier backend identity systems, the EUDIW is a user-facing application,

demanding a shift in certification paradigms (Schwalm & Alamillo-Domingo, 2021). Certification must not only confirm technical compliance but also reinforce user trust and foster cross-border acceptance.

Achieving certification consistency across all EU member states is essential. Without standardized approaches, national inconsistencies could lead to fragmentation and undermine the EUDIW's interoperability goals (Sharif et al., 2022). Divergent certification practices may also hinder citizen adoption, as public trust is closely linked to perceptions of security and reliability (Podgorelec et al., 2022). The importance of addressing these risks has been emphasized by studies highlighting the role of citizen trust in the success of eID systems (Davis, 1989; Lee et al., 2003).

Emerging technologies such as blockchain, zero-knowledge proofs and decentralized identifiers present both opportunities and challenges for certification schemes. These technologies can significantly enhance security and privacy but introduce new governance and technical risks (Morosi, 2022). Research by Fernández (2024) has pointed out that improperly regulated blockchain-based identity systems may compromise privacy if not carefully designed. Regulatory adaptability, therefore, becomes a key factor in ensuring that certification remains relevant as technological paradigms shift (Gallo et al., 2014**).**

Estonia offers a unique reference point for understanding how national ecosystems can adapt to these evolving challenges. With its highly developed eID infrastructure, proactive participation in EU digital initiatives and experience with cross-border service delivery frameworks like the Single Digital Gateway (SDG), Estonia serves as a model for successful digital identity management (e-Estonia, 2024; Aavik & Krimmer, 2016). The importance of aligning national practices with EU-wide frameworks, such as the Once-Only Principle, has been further underscored by research into cross-border interoperability (European Parliament & Council of the European Union, 2022; Kalvet et al., 2018).

Governance and institutional design theories provide a valuable lens for understanding how certification frameworks can balance national autonomy and EU harmonization (Williamson, 1998; Koppenjan & Groenewegen, 2005).

Addressing the challenges associated with EUDIW certification is critical for achieving a resilient, trustworthy, and interoperable European digital identity landscape. Efforts must focus on establishing certification frameworks that are adaptable to technological innovation, legally robust, and capable of fostering cross-border mutual recognition and user trust.

Some sections of this thesis incorporate content from the master's student's own work in ITE4260 Research Methods (Spring 2024) and ITE4310 E-Governance Technologies and Services Master's Project (Autumn 2024). In line with principles of academic integrity and transparency, the author discloses the use of certain AI tools in the preparation of this thesis. ChatGPT 4o[1] was used to explore topic formulations and reorganize sections for coherence. Grammarly[2] and Wordtune[3] were used to review and improve grammar and wording. No AI-generated text was used without substantial revision and review by the author.

1.1 Research purpose

This thesis aims to support the development of a national certification scheme for the European Digital Identity Wallet (EUDIW) by proposing a conceptual framework that ensures alignment with the revised eIDAS Regulation and strengthens institutional preparedness across EU member states. The research aims to contribute to a structured certification model that accommodates national governance requirements while aligning with pan-European legal, technical and procedural expectations.

The conceptual framework seeks to address the lack of established national-level certification schemes by offering practical guidance and governance components, supporting both immediate implementation needs and long-term adaptability. Emphasis is placed on ensuring trust, interoperability and regulatory clarity to facilitate the secure rollout of EUDIW across diverse institutional environments. Through this, the study aims

[1] https://chatgpt.com/

[2] https://app.grammarly.com/

[3] https://app.wordtune.com/

to promote consistent standards for wallet certification and offer a transferable model that can inform policymaking beyond the Estonian context.

1.2 Research motivation

The motivation for this study comes from a combination of academic interest and practical need. As a student of E-Governance Technologies and Services, the author has been exposed to the policy, technical and societal dimensions of digital identity. To complement this academic background with practical insight, the author also took part in the *EU Digital Wallet Workshop* held on 8 May 2025 in Tallinn, Estonia. Estonia's leadership in digital public services and its strategic position in European digital integration offer a compelling context for deeper inquiry.

The rollout of the EUDIW across all EU member states by the end of 2026 represents a unique opportunity, but also a major risk, if not implemented cohesively. With implemention acts adopted and pilot projects underway, time is of the essence. The certification component is particularly underdeveloped yet foundational to ensuring interoperability, legal compliance and user trust. The author recognized that despite strong policy ambition at the EU level, significant knowledge gaps exist regarding how national certification schemes should be designed and operationalized in practice.

Furthermore, the research addresses pressing questions around auditability, institutional responsibility and agile regulation, all of which are essential to long-term success. The goal is to produce a framework that addresses Estonia's needs and serves as a model for other countries navigating similar challenges.

1.3 Research questions

This study aims to propose a conceptual framework for developing a national certification scheme for the EU Digital Identity Wallet (EUDIW). The primary focus will be on designing a certification framework that meets the specific requirements of the EUDIW, considering current assessment practices, identifying key certification criteria and aligning with national and EU standards.

To achieve this objective, the following Research Question (RQ) and Sub Questions (SQ) were drafted:

RQ1. How to develop the national EUDI wallet certification scheme?

SRQ1. What are the current assessment requirements for eID schemes?

SRQ2 What are the EUDIW certification requirements?

SRQ3. What is the correlation between the current eIDAS implementation assessment practise and EUDIW certification requirements?

SRQ4. What are the key factors for designing the EUDIW certification framework?

SRQ5. What are the challenges in implementing the EUDIW certification scheme?

One main research question and relevant sub-questions will be answered through the analysis of technical and legal documentation, qualitative expert interviews and the integration of relevant theoretical context. The findings from this research will lead to policy suggestions and conclusions at both the EU and national levels to aid in decision-making within this rapidly changing area.

1.4 Thesis outline

This thesis is structured into ten chapters that guide the reader from the foundational context of the European Digital Identity Wallet (EUDIW) to the development of a national certification framework proposal. The first chapter introduces the background of the study, outlines the research purpose, motivation, research questions and provides an overview of the thesis structure. The second chapter reviews the evolution of the eIDAS regulation, digital identity frameworks in Europe and key academic discussions on certification, interoperability and emerging technologies relevant to the EUDIW. The third chapter provides the contextual background, reviewing the current state of eIDAS and EUDIW standardization, the role of implementing acts, key certification requirements and Estonia's position and readiness for wallet implementation. The fourth chapter introduces the theoretical foundations of the study, drawing from Williamson's institutional analysis model and the institutional governance approach by Koppenjan and Groenewegen to form an integrated framework for analysing certification systems. The

fifth chapter explains the research methodology, including the qualitative case study design, data collection methods through expert interviews and document analysis and the thematic analysis approach used to interpret findings. In the sixth chapter, the author presents the results of the expert interviews, thematically organized to cover EU-level implementation, national challenges, technological and regulatory alignment, and institutional readiness. The seventh chapter offers a discussion that synthesizes the findings with the theoretical frameworks and concludes with policy recommendations for Estonia and other member states. The eighth chapter presents the author's main contribution, a conceptual framework for national EUDIW certification, developed by integrating empirical insights with institutional design principles. The ninth reflects on the limitations of the study and proposes future research directions, including comparative case studies and technical prototyping. The final, tenth chapter summarizes the main contributions of the thesis, reinforcing the need for a governance-driven, adaptable and scalable certification model for EUDIW implementation.

2 Literature Review on European Digital Identity Frameworks

The governance of digital identity frameworks in the European Union relies on two interrelated but distinct processes: standardization and certification. Standardization refers to the establishment of uniform technical and regulatory specifications to ensure interoperability across digital identity systems, whereas certification is a formal process that validates compliance with those standards (Turner, 2003). These mechanisms play a crucial role in ensuring trust, security, and cross-border functionality in digital identity frameworks (Matus, 2009). This distinction is particularly relevant when considering the development of the European Digital Identity Wallet (EUDIW), as its successful implementation depends on both standardized frameworks and an effective certification model.

This chapter presents an overview of existing literature on European digital identity frameworks, with an emphasis on the European Digital Identity Wallet (EUDIW). It examines academic insights and highlights areas where research is still lacking, particularly in relation to developing a national certification framework. To provide a well-rounded perspective, this review also considers contrasting viewpoints on the impact of digital identity standardization, ensuring a balanced discussion. The discussion situates the EUDIW within the broader context of digital identity and trust services within the European Union. Given the focus on cross-border digital identity services, the analysis prioritizes scholarly work relevant to the unique regulatory and technical challenges faced within the European region.

The review is based on sources retrieved from academic databases such as ScienceDirect, SSRN, ResearchGate and Google Scholar. To ensure a systematic selection of sources, relevant search keywords such as “European Digital Identity Wallet,” “eIDAS,” “eIDAS 2.0,” “digital identity certification,” and “cross-border interoperability” were used. To maintain relevance, the scope of the literature is limited to works published after 2014,

following the implementation of the eIDAS Regulation (*Regulation (EU) No 910/2014*, 2014), which established a legal framework for electronic identification and trust services across the EU.

2.1 Literature on eIDAS Regulation and its impact

The eIDAS Regulation (*Regulation (EU) No 910/2014*, 2014) marked a significant milestone in the establishment of secure, interoperable digital identity systems and set the stage for subsequent advancements like the EUDIW. Initially implemented in 2014, eIDAS established a unified framework for electronic identification (eID) and trust services, enabling secure cross-border recognition of eID systems. Studies by Czerny et al. (2023) and Schwalm (2023) highlight the regulation's pivotal role in standardizing digital identification processes, empowering users with legally recognized digital tools like traditional physical documents. This standardization has unlocked numerous digital opportunities across sectors, from e-government services to e-banking, emphasizing the importance of interoperability for seamless integration across member states (European Commission, 2021). Digital identity has consistently been viewed as essential for enabling secure and dependable communications between different parties (Mazzocca et al., 2024).

Despite these benefits, scholars argue that the one-size-fits-all approach of eIDAS does not sufficiently account for the differing digital maturity levels of member states (Berbecaru et al., 2019). Countries with advanced digital infrastructures have integrated eIDAS relatively seamlessly, whereas others face resource constraints and technological gaps, limiting their ability to comply effectively. The role of digital maturity in influencing the effectiveness of standardization remains a key area for further research.

While standardization is widely regarded as essential for interoperability (Sedlmeir et al., 2021), some scholars argue that rigid frameworks can hinder technological innovation and adaptability across diverse national infrastructures (Doshi & Schmidt, 2024). This raises the central debate surrounding standardization: its necessity for ensuring security and interoperability versus its potential to limit flexibility in a rapidly evolving technological landscape.

Another key discussion in the literature concerns certification models in digital identity governance. Some scholars advocate for a fully centralized EU-level certification approach, ensuring uniform security and compliance measures across all member states. Others, however, argue for a decentralized model, where national authorities retain flexibility in defining security and compliance frameworks tailored to local circumstances (Schwalm & Alamillo-Domingo, 2021). The ongoing debate highlights the tension between achieving interoperability and allowing regulatory adaptability across diverse digital landscapes. Further research is needed to evaluate how these models impact digital identity governance at both the national and EU levels.

2.2 Literature regarding European digital identity framework

The revision of eIDAS through eIDAS 2.0 introduces the European Digital Identity Wallet (EUDIW), which is expected to transform the digital identity landscape across Europe (*Regulation (EU) 2024/1183*, 2024). This amendment requires all member states to develop and certify their digital identity solutions, ensuring seamless access to cross-border services (Steffen, 2023). The EUDIW is designed to simplify and secure a wide range of digital interactions, covering e-government services, e-health and even e-commerce to foster a more integrated digital ecosystem across the EU (Council of the European Union, n.d.).

While eIDAS 2.0 enhances security and user control over digital identities, some researchers argue that it may introduce new compliance burdens for both public and private-sector service providers. Busch (2022) highlights that increased regulatory requirements could result in financial and legal uncertainties, particularly for private companies where identity verification is a core aspect of service delivery. Further research is needed to assess the cost implications and legal challenges associated with implementing eIDAS 2.0.

In the context of the European Digital Identity Wallet (EUDIW), certification plays a crucial role in ensuring regulatory compliance across member states. Schwalm and Alamillo-Domingo (2021) warn that, without a clear certification framework, the EU risks creating a fragmented landscape where national standards diverge, ultimately undermining the interoperability objectives of eIDAS 2.0.

Given these regulatory complexities, certification plays a crucial role in ensuring compliance and interoperability across member states. However, the lack of a unified approach has sparked debate. Some researchers propose the establishment of a centralized EU-level certification body to ensure compliance with digital identity standards across all member states, while others argue for a hybrid model where national regulators maintain some oversight while aligning with EU-wide standards (Sharif et al., 2022). Without clear certification guidelines, national standards risk diverging, undermining the interoperability goals of eIDAS 2.0. This regulatory uncertainty remains a challenge, and further research is needed to assess the feasibility of different certification models for the EUDIW.

The role of emerging technologies in digital identity has also been widely discussed. Blockchain, artificial intelligence (AI) and zero-knowledge proofs offer new possibilities for enhancing security and privacy in digital identity systems (Morosi, 2022; Fernández, 2023). However, integrating these technologies within the eIDAS framework introduces new governance and security challenges. Fernández (2024) highlights the risks associated with blockchain-based digital identity solutions, particularly in terms of security vulnerabilities if not properly regulated. Additionally, ambiguity in the eIDAS 2.0 regarding mandated technological standards complicates compliance with regulations such as GDPR and raises concerns about interoperability with other emerging solutions (Sharif et al., 2022; Nakashidze, 2023).

To address these uncertainties, researchers suggest exploring regulatory sandboxes or pilot programs, which could offer valuable insights into how new technologies can be integrated while maintaining regulatory compliance. This approach would help assess the practical viability of different digital identity models under real-world conditions.

The literature highlights the importance of developing a national certification scheme for the EUDIW to ensure security, standardization, and interoperability across Europe's digital identity systems. While eIDAS 2.0 sets ambitious goals for digital identity in the EU, questions remain regarding the long-term sustainability of the certification model and its impact on both public and private stakeholders.

This chapter has not only examined the body of work surrounding the EUDIW but also situated it within the broader discussion about digital identity standardization, certification requirements and cross-border service integration in Europe. The analysis highlights gaps in existing knowledge and underscores the importance of further research to guide the development of national certification frameworks aligned with the goals of eIDAS 2.0.

3 Research background

As the European Union continues its path toward greater digital integration, the introduction of the European Digital Identity Wallet (EUDIW) under the revised eIDAS 2.0 Regulation represents a major milestone in the development of secure, interoperable cross-border services. Building upon the foundation laid by eIDAS (*Regulation EU No 910/2014*, 2014), the EUDIW is expected to enable EU citizens, residents and businesses to securely store and share verified digital credentials for use in both public and private sector interactions. Unlike previous identification schemes, the EUDIW brings a comprehensive approach by integrating identity data, electronic attestations and authentication capabilities in a single digital wallet governed by a harmonised European framework.

However, as EU member states begin to implement this novel solution, questions of certification, interoperability and legal compliance become central to its success. The shift from certifying individual services to certifying entire wallet ecosystems introduces new challenges related to governance, technical standards and privacy safeguards.

3.1 eIDAS and EUDIW standardisation

3.1.1 eIDAS overview

The eIDAS Regulation (*Regulation EU No 910/2014*, 2014), introduced in 2014, marked a transformative step towards enabling secure and seamless digital interactions across EU member states. Its primary objective was to standardize the legal recognition of electronic identification and trust services such as e-signatures, e-seals, timestamps and website authentication. By doing so, it laid the foundation for the mutual recognition of national eID schemes across borders, enabling users to access public services digitally in any EU country using their own national eID. As of 2025, the regulation has played a critical role in expanding the Digital Single Market and facilitating cross-border digital transactions.

However, the original eIDAS framework presented several challenges. Notably, it left much discretion to member states regarding implementation, leading to divergent levels of adoption and digital maturity. Countries like Estonia made rapid advancements in integrating their eID solutions, while others struggled with technical or policy limitations. The lack of a unified, EU-wide identity solution also left a gap in usability and user control. These limitations prompted a substantial revision of the regulation, culminating in the adoption of eIDAS 2.0 in 2024.

3.1.2 Current certification landscape

The certification landscape in the context of eIDAS (electronic IDentification, Authentication and trust Services) and the European Digital Identity Wallet (EUDIW) is a dynamic and evolving domain, shaped by ongoing regulatory reforms, technological innovations and the growing demand for secure and interoperable digital identity systems. This section provides an overview of the development path and current challenges in certification under the revised eIDAS 2.0 framework.

The original eIDAS Regulation (*Regulation EU No 910/2014*, 2014) served as a cornerstone for establishing trust in digital interactions across the European Union by providing a common legal framework for electronic identification and trust services (European Commission, 2014). It facilitated cross-border interoperability and introduced the certification of Qualified Trust Service Providers (QTSPs), who are authorized to issue qualified certificates for electronic signatures, seals, timestamps and delivery services. The certification process for QTSPs includes a conformity assessment conducted by accredited bodies, issuance of qualified certificates and continuous supervision by national regulatory authorities (Nguyen, 2018).

The 2021 proposal to revise the eIDAS Regulation resulted in Regulation (EU) 2024/1183, marking a significant turning point in the European digital identity landscape (European Commission, 2024f). The updated regulation introduced the EUDIW as a new layer within the digital identity landscape, allowing individuals to store and use verified credentials in a secure, cross-border environment (European Commission, 2024g). This shift called for new certification approaches, rather than focusing solely on individual services like e-signatures, certification now extends to entire wallet ecosystems that must

meet rigorous standards for security, privacy, usability and interoperability (European Union Agency for Cybersecurity, 2024).

To guide this process, the European Commission adopted five Implementing Acts in November 2024. These acts define the technical protocols, certification procedures, notification obligations and rules for identity data and credential management in the EUDIW ecosystem. The regulations: Commission Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980, 2024/2981 and 2024/2982, create a harmonised legal and procedural framework for the wallet certification process across EU member states (European Commission, 2024a–e). A summary of their focus areas is presented in Table 1 below.

Table 1. Overview of eIDAS 2.0 Implementing Acts relevant to EUDIW Certification

Regulation	**Focus Area**
Commission Implementing Regulation (EU) 2024/2977	Issuance of person identification data and electronic attestations of attributes
Commission Implementing Regulation (EU) 2024/2979	Protocols and interfaces for wallet technical operations
Commission Implementing Regulation (EU) 2024/2980	Notification procedures for ecosystem stakeholders
Commission Implementing Regulation (EU) 2024/2981	Certification procedures for digital identity wallets
Commission Implementing Regulation (EU) 2024/2982	Additional technical and procedural specifications

Compiled from European Commission Implementing Regulations published in the Official Journal on 28 November 2024. See: European Commission (2024a, 2024b, 2024c, 2024d, 2024e).

Under the new framework, certification processes must now address additional layers of complexity. This includes verifying wallet architecture, cryptographic integrity, biometric or multifactor authentication, selective disclosure capabilities and privacy-by-design requirements (Seegebarth et al., 2024). The goal is not only to ensure regulatory compliance but also to guarantee that the EUDIW functions securely and consistently across various national ecosystems.

Despite these advancements, challenges persist. The implementation of EUDIW certification mechanisms remains uneven across member states due to disparities in national legislation, technological maturity and administrative readiness (Andrade, 2023). Moreover, interoperability remains a pressing concern. While eIDAS seeks to harmonize

digital identity frameworks, varying national standards for electronic identification and certification may create bottlenecks in cross-border service delivery (Mocanu et al., 2019).

Additionally, the success of the European Digital Identity Wallet (EUDIW) depends on widespread user adoption, which in turn depends on trust in the wallet's security and usability. To encourage citizens to use digital wallets for sensitive interactions, such as healthcare access, tax declarations or banking, the certification framework must effectively address privacy, data control and resilience against cyber threats. The European Union Agency for Cybersecurity (ENISA) is actively developing a cybersecurity certification scheme for EUDI Wallets to ensure they meet stringent security and privacy standards, thereby fostering user confidence and facilitating cross-border acceptance within the EU (European Union Agency for Cybersecurity, 2024).

Looking ahead, the path of certification within eIDAS 2.0 will likely be shaped by further regulatory refinement and technological advancements. Innovations such as blockchain, artificial intelligence and even quantum-resilient encryption may redefine trust models and assurance mechanisms (Nguyen, 2018; Soler, 2018). Moreover, global digital trade and mobility may prompt further alignment between EU frameworks and international standards (European Commission, 2024i).

3.1.3 Key factors for certification design: security, privacy, technology, and compliance

The design of a national certification framework for the European Digital Identity Wallet (EUDIW) must be grounded in four core pillars: security assurance, privacy protection, technological alignment and regulatory compliance. Together, these dimensions ensure the trustworthiness, interoperability and resilience of digital wallets across EU member states.

Security is foundational for certification. The framework must adhere to internationally recognized standards such as ISO/IEC 27001, the NIST Cybersecurity Framework and sector-specific guidance from ENISA (ENISA, 2023; NIST, 2024). These standards help manage systemic risk, define best practices for secure information handling and prepare systems to resist evolving cyber threats. In addition, assurance models such as ISO/IEC

29115 offer classification for identity proofing and authentication levels, relevant for assessing the integrity of digital identity wallets (ITEH, 2024).

Privacy is equally critical, especially under the scope of the General Data Protection Regulation (GDPR). Certification criteria must ensure compliance with privacy-by-design and privacy-by-default principles. Requirements include data minimization, explicit user consent, secure storage of personal data and the application of privacy-enhancing technologies such as zero-knowledge proofs, which allow for credential verification without revealing unnecessary information (Fernández, 2024).

Technological alignment ensures that certified wallets integrate seamlessly with both national infrastructures and pan-European systems. EUDIW certification must account for compatibility with legacy systems and support for emerging technologies like AI-powered authentication, decentralized identifiers (DIDs) and modular architectures. API standardization and forward-compatibility are essential for scalability and cross-border usability (Sharif et al., 2022; Morosi, 2022).

Lastly, regulatory compliance must reflect both EU-wide requirements and domestic legislation. The Implementing Acts of November 2024 define the technical specifications, credential types, wallet issuance procedures and governance expectations under eIDAS 2.0 (European Commission, 2024h). National certification schemes must align with these provisions while ensuring feasibility for conformity assessment bodies (CABs) and wallet providers to implement them effectively.

In summary, these four pillars provide a structured foundation for developing certification schemes that are not only compliant and secure but also future-proof and interoperable within the broader EUDIW ecosystem.

3.2 European Digital Identity Wallet Overview

The European Digital Identity Wallet (EUDIW) represents a significant evolution in the EU's approach to digital identity, aiming to address the limitations of the original eIDAS regulation and to meet the rising demand for secure, interoperable and user-centric digital identity tools. Established in the framework of the revised eIDAS 2.0 Regulation

((European Commission, 2024f), the EUDIW is designed to become a core enabler of cross-border online service delivery across all EU member states by the end of 2026. By 2027, all public and private sector service providers that are legally required to use strong user authentication must accept EUDI Wallets as a means of identification (*Regulation (EU) 2024/1183,* 2024).

The EUDIW will be available to any EU citizen, resident, or business that wishes to use it. It allows users to securely store, manage and share personal identification data and verifiable credentials, such as educational qualifications, mobile driving licenses and health records, with both public institutions and private-sector platforms like banks and healthcare providers. According to the European Commission (2024j), this tool is not only universally accessible but also under the user's control, ensuring compliance with the General Data Protection Regulation (GDPR) and the sole user control requirement set out in Article 5a(4)(a) of eIDAS 2.0 (*Regulation (EU) 2024/1183*, 2024).

The EUDIW complements rather than replaces existing national eID systems by enhancing their cross-border operability (Mölder, 2024). It is built upon a mobile-first architecture and modular design, leveraging the Architecture and Reference Framework (ARF) from the EU Digital Identity Toolbox (European Commission, 2024k). The ARF supports interoperability through standardized APIs and a decentralised trust model, ensuring alignment with national infrastructures and EU-wide standards (European Commission, 2024j).

The ARF defines the roles, interactions, and governance responsibilities across the EUDI Wallet ecosystem. It includes EUDI Wallet Providers, PID Providers, Qualified Electronic Attestation of Attributes (QEAA) Providers, Relying Parties, and supervisory bodies. These roles are interconnected through a layered trust and registration model, facilitating secure, scalable, and user-controlled identity management across borders. Figure 1 illustrates a more detailed structure of interactions within the eIDAS 2.0 architecture reference framework, focusing on different providers and their roles.

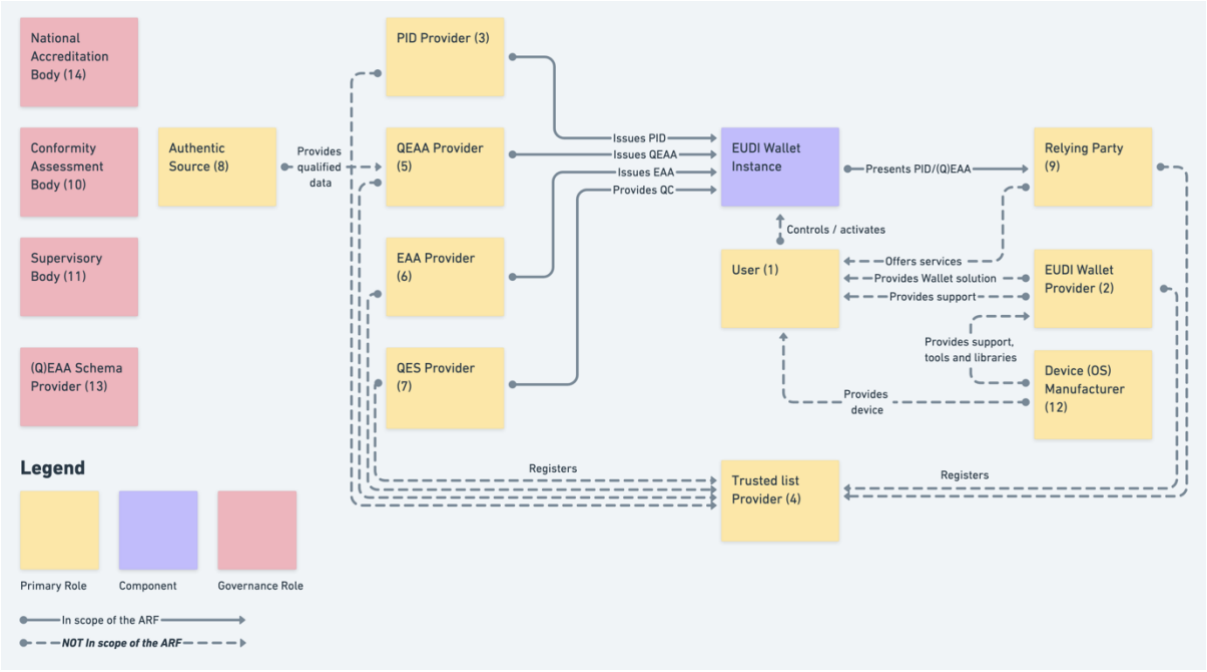

Figure 1. EUDI Wallet roles and connection based on the Architecture and Reference Framework (ARF). Taken fully form: European Commission (2024j)

Security within this ecosystem is achieved through mechanisms such as trusted device certification, secure key storage and identity binding protocols. For example, wallets must integrate with device secure elements or Trusted Execution Environments (TEEs) to ensure private keys and credentials are protected against tampering. Additionally, interactions between entities (e.g., between PID Providers and Wallets) rely on mutual authentication, digitally signed attestations, and strict adherence to technical specifications defined in the ARF (European Commission, 2024j).

A key challenge for the EUDIW lies in establishing a certification framework that ensures wallets meet common security and interoperability standards while remaining adaptable to varied implementation models. Certification must support both public and private wallet issuers and provide assurance for end users and service providers across the EU. This includes technical conformance, data protection safeguards and operational governance standards.

Regional cooperation efforts offer valuable insights in this regard. The Nordic-Baltic eID (NOBID) consortium is one of the most prominent cross-border pilots, involving countries such as Norway, Denmark, Iceland, Latvia, Germany and Italy. Focused on

enabling payments and other real-world transactions with EUDIW-based wallets, NOBID demonstrates how mutual recognition and interoperable trust frameworks can be achieved in practice (NOBID Consortium, 2023; European Commission, 2024g).

This initiative also illustrates the value of public-private collaboration. Organizations like Poste Italiane contribute technical and organizational expertise in digital onboarding and wallet deployment, helping to shape certification schemes that are practical, scalable and aligned with market needs (Poste Italiane, 2024).

Ultimately, the EUDIW must interoperate with broader EU digital infrastructure initiatives such as the Single Digital Gateway. Its success will depend on the ability to coordinate standards, foster institutional trust and resolve both technical and legal complexities. If implemented effectively, the EUDIW has the potential to become a unifying foundation for secure digital identity and service access across Europe.

3.3 Estonian eID and EUDI Wallet Implementation Status

Estonia has long been considered a pioneer in digital identity, with its strong national infrastructure enabling the secure and convenient use of eID solutions across society. As the European Union moves toward introducing the European Digital Identity Wallet (EUDI Wallet), Estonia is building on its existing ecosystem to become one of the first countries to develop and implement a compliant solution. The revised eIDAS regulation, expected to apply from 2026 onwards, requires Member States to offer a wallet that supports high-assurance electronic identification and trust services across borders. Estonia's approach reflects its strategic commitment to interoperability, privacy and user-centric digital governance.

3.3.1 Current eID ecosystem and roles

Estonia's leadership in digital identity is reflected in its mature eID ecosystem, which has evolved over two decades of innovation and public trust. Its eID system is supported by a well-established infrastructure comprising the national ID card, Mobile-ID, Smart-ID and more recently, biometric authentication solutions. The architecture relies on strong encryption, Public Key Infrastructure (PKI), and the secure data exchange platform X-

Road, which underpins many public services and enables seamless, secure information sharing across institutions (Kawamura, 2023; Cybernetica, 2023).

Key institutional actors include the Information System Authority (RIA), which oversees the development and maintenance of national digital services and authentication mechanisms such as TARA (Trusted Authentication and Recognition Architecture). RIA also plays a central role in coordinating Estonia's response to the updated eIDAS regulation and leads the development of the EE Wallet. Responsibility for electronic identification, which was formerly under the Ministry of Economic Affairs and Communications (MKM), has been reassigned to the newly established Ministry of Justice and Digital Affairs (JUSTDIGI), which now leads national efforts related to eID and ensures alignment with European Union digital identity frameworks and strategies.

SK ID Solutions is a major trust service provider and certification authority that issues certificates for Mobile-ID and Smart-ID and is recognized under the eIDAS framework. The Estonian Police and Border Guard Board (PPA) is tasked with issuing identity documents and plays a key role in ensuring the reliability of identity attributes linked to the eID ecosystem. These entities collaborate within a governance framework that supports transparency, technical resilience, and regulatory compliance (Kawamura, 2023; Cybernetica, 2023).

3.3.2 EUDI Wallet status in Estonia

Estonia is actively preparing for the implementation of the European Digital Identity Wallet (EUDI Wallet) in line with the revised eIDAS regulation. While Estonia is considered a frontrunner in digital identity, it does not plan to develop the national wallet solution in-house. Instead, the approach foresees procuring the wallet as a service from an external provider. The Information System Authority (RIA) is coordinating national preparations and is expected to take on the role of Wallet Provider, ensuring that the selected solution meets the required Level of Assurance (LoA High) as mandated by eIDAS 2.0 (Cybernetica, 2023).

The Estonian EUDI Wallet, referred to as the EE Wallet, is designed to function as a high assurance eID means, supporting secure authentication and selective disclosure of identity attributes. It will enable use in both online and offline contexts, integrating

capabilities like biometric verification and cryptographic proofs for identity binding. A strong emphasis is placed on user convenience and accessibility, the wallet is intended to be activated using only an ID card and an NFC (Near Field Communication) capable smartphone, eliminating the need for desktop computers or card readers (Cybernetica, 2023).

While the Estonian Police and Border Guard Board (PPA) is responsible for issuing physical identification documents, the authoritative source of Person Identification Data (PID) is the national Population Register, which is managed by the Ministry of the Interior. In the context of the EUDI Wallet, the *Digikukru* analysis (Cybernetica, 2023) assumes that PPA could act as the PID Provider, given its existing role in face-to-face identification and document issuance. However, this institutional setup has not been confirmed and alternative models, such as assigning the role to RIA, a trust service provider, or a hybrid arrangement, remain under consideration and would require a political decision. Estonia's design considerations also reflect growing privacy concerns. The EE Wallet is expected to rely initially on long-term PID attestations (e.g., five-year validity, like current ID card certificates), but there have been discussions around implementing short-term attestations to better support anonymous authentication and mitigate profiling risks.

Estonia is an active participant in the eIDAS Expert Group, contributing to the development of the European Digital Identity Wallet Architecture and Reference Framework (ARF). As such, the EE Wallet will conform to standards such as W3C Verifiable Credentials and ISO/IEC 18013-5, ensuring cross-border interoperability. Development is currently in a prototype and analysis phase, involving architecture design, interface specifications and detailed process modelling. The EE Wallet will be integrated into the country's broader digital infrastructure, leveraging platforms such as TARA and X-Road for secure service delivery (Cybernetica, 2023).

In parallel to technical development, legal preparedness remains a crucial consideration. Õunapuu (2024) points out several shortcomings in Estonian legislation, particularly regarding the limited clarity around the supervisory responsibilities for trust services and the lack of resilience planning for critical QTSP dependencies. Her thesis recommends

legal updates to better align with the anticipated requirements under eIDAS 2.0 and the Critical Entities Directive (pp. 36–39).

In conclusion, Estonia is well-positioned for the rollout of the EUDI Wallet. By leveraging its mature digital identity infrastructure and strong governance, the country is shaping a solution that not only meets EU requirements but also enhances privacy, usability, and trust in digital services. However, this same well-established ecosystem also presents integration challenges, as the legacy systems and institutional structures may complicate the introduction of new solutions within the existing framework.

4 Theoretical frameworks

This study applies a multi-framework theoretical approach to understand how national certification systems for the European Digital Identity Wallet (EUDIW) can be structured and governed. Given EUDIW's complexity and multi-actor landscape, a layered and design-oriented perspective is necessary to capture the institutional, procedural and technical dynamics shaping certification at the national level.

More specifically, this study employs Koppenjan and Groenewegen's (2005) institutional design model, which builds upon and extends Williamson's (1998) four-level framework of institutional analysis. The integration of these perspectives provides a comprehensive analytical lens to examine how informal norms, formal institutions, governance structures and technological implementations interact to shape certification systems under the EUDIW initiative.

This chapter is structured into three parts. First, Williamson's layered model is introduced to capture the temporal and hierarchical nature of institutional change. Second, Koppenjan and Groenewegen's model offers a governance-oriented perspective on shaping institutional, technological and procedural design. Third, the models are synthesized into a combined framework tailored to the EUDIW certification context.

4.1 Williamson's Layered Institutional Framework

Williamson's (1998) institutional analysis model offers a foundational perspective for examining how institutional environments affect system design, compliance and long-term adoption. It decomposes institutional evolution and decision-making into four interconnected levels.

At the top of the hierarchy, the fourth layer represents the informal institutional environment. Informal institutions refer to deeply embedded societal values, norms and cultural orientations. These change slowly over time and form the foundation of

legitimacy and trust in any governance system. In the context of EUDIW, this layer influences citizen acceptance of the wallet and the broader trust framework within which certification is carried out.

The third layer comprises the formal institutional environment, consisting of constitutions, legal systems, public policies and regulations. These elements define the legal frameworks for governance and certification. For EUDIW, this includes instruments such as the eIDAS 2.0 regulation and national legislation that transposes EU-level requirements into domestic law, ensuring legal interoperability across member states.

Moving to the second layer, institutional arrangements capture the formal and informal agreements between actors that shape coordination and cooperation. These include contracts, memoranda of understanding, procedural guidelines and governance protocols. In the case of EUDIW certification, this layer encompasses the working relationships among the European Commission, national authorities and conformity assessment bodies, ensuring strategic alignment and procedural clarity.

At the base, the first layer focuses on actors and their interactions within the socio-technical system. This includes the daily operations, resource allocations and implementation practices that embody institutional rules and objectives. For EUDIW, this involves the technical realization of the digital wallet, including cryptographic mechanisms, user interface integration and compliance testing infrastructure.

This layered structure provides a powerful analytical lens for understanding how effective certification systems must align high-level societal values with legal mandates, governance routines, and concrete technological execution. Figure 2 illustrates Williamson's four-layer institutional model, highlighting how different levels of institutional structures interact to shape system behaviour and long-term stability:

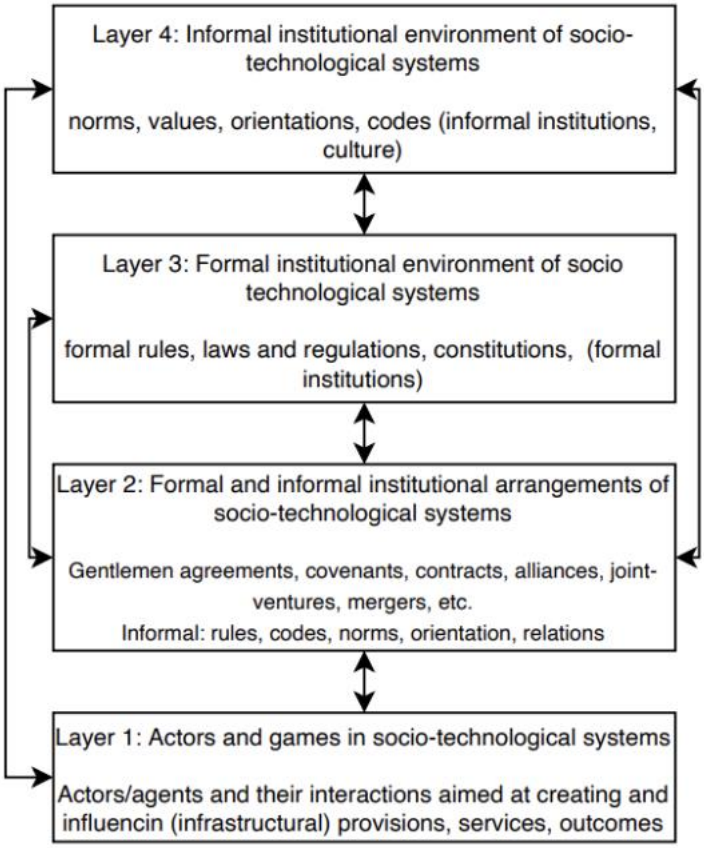

Figure 2. Four-Layer Institutional Analysis Model

Source: Williamson (1998)

4.2 Institutional Governance Approach (Koppenjan and Groenewegen)

The institutional governance model proposed by Koppenjan and Groenewegen (2005) provides a design-oriented extension to Williamson's layered institutional framework. While Williamson helps explain the structural and time-based dynamics of institutional change, Koppenjan and Groenewegen offer a practical lens through which to organize and steer complex governance systems. Their model can be viewed as operating horizontally across Williamson's layers focusing on how institutional, technological and process design can be deliberately structured to influence outcomes across all levels of the institutional hierarchy.

This approach is particularly relevant for shaping the certification framework of the European Digital Identity Wallet (EUDIW), where coordination between EU institutions,

national governments, private sector actors and citizens is essential. The successful implementation of the EUDIW certification framework at national level requires robust institutional design that integrates regulatory alignment, technological architecture and procedural oversight.

Koppenjan and Groenewegen argue that digital infrastructures such as the EUDIW depend on governance systems capable of managing uncertainty, coordinating diverse interests and adapting to evolving technical and legal contexts. Their framework identifies three interdependent governance components: institutional arrangements, technological design and process design. These components interact continuously and must be developed in alignment to ensure the EUDIW's successful certification and implementation.

This framework is particularly valuable in the context of cross-border digital identity governance, where national certification processes must comply with European-level standards while maintaining flexibility for domestic implementation. Figure 3 presents a conceptual representation of how institutional; technological and process design interrelate to structure governance in digital infrastructure systems.

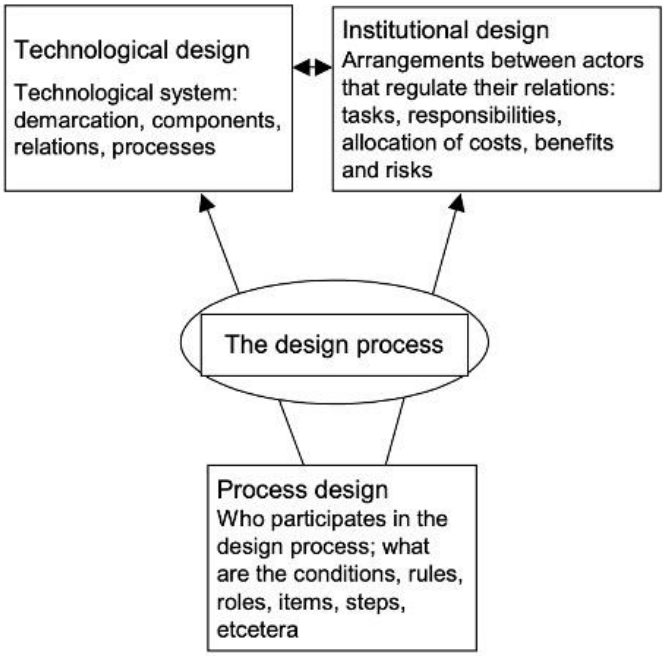

Figure 3. Institutional design positioning.

Source: Koppenjan and Groenewegen (2005)

This figure highlights the importance of simultaneous attention to formal structures, technical systems and procedural rules when designing national certification frameworks that support both EU-level interoperability and local trust and functionality.

4.2.1 Institutional arrangements and regulatory framework

Institutional arrangements refer to the legal, organizational and regulatory structures that define the roles and responsibilities of different actors within a complex system. According to Koppenjan and Groenewegen (2005), institutional arrangements help manage multi-actor networks and provide stability and coordination mechanisms for complex technological systems.

For EUDIW certification, institutional arrangements must structure the relationships between public and private actors to ensure secure and interoperable digital identity services. The legal foundation for these arrangements is provided by the revised eIDAS 2.0 Regulation (*Regulation (EU) 2024/1183*, 2024), which introduces the European Digital Identity Wallet and establishes common rules for its issuance, certification, and supervision across Member States. The regulation outlines the roles of EU-level institutions, such as the European Commission and ENISA, as well as national wallet issuers, conformity assessment bodies and supervisory authorities.

Koppenjan and Groenewegen emphasize that institutional frameworks should reduce uncertainty and facilitate strategic risk-sharing among actors. In the context of EUDIW certification, a clear definition of roles between EU-level authorities (such as the European Commission), national wallet issuers, and certification bodies is critical to maintaining trust and ensuring transparency across jurisdictions.

4.2.2 Technological design and standardization in certification

Technological design plays a crucial role in the governance of complex systems by ensuring that technical infrastructures support coordination among multiple actors. According to Koppenjan and Groenewegen (2005), technological design must be aligned with institutional structures to ensure that systems remain stable, scalable and adaptable to evolving conditions.

In the EUDIW case, this refers to architectural components like reference wallets, cryptographic standards, biometric security and interfaces with national ID schemes. The design must accommodate cross-border operability while integrating with varying national infrastructures.

4.2.3 Process design and institutional adaptation

Process design refers to the mechanisms by which governance structures evolve and are operationalized. In EUDIW certification, this includes stakeholder engagement, conformity assessment routines, audit procedures and mechanisms for iterative policy revision.

A well-designed process structure ensures that the certification system remains responsive to legal, technological and societal changes. It also fosters inclusion, transparency and learning, which are vital for long-term trust and system effectiveness.

This design-centric approach provides actionable guidance for shaping EUDIW governance systems that are robust, flexible and institutionally sound, preparing them for the challenges of pan-European implementation.

These three components institutional, technological and process design offer a governance-oriented perspective on system architecture. The following section integrates this lens with Williamson's institutional layering to form a combined framework tailored for EUDIW certification.

4.3 Combined governance lens for EUDIW certification

The integration of Williamson's layered institutional model with Koppenjan and Groenewegen's governance architecture offers a multidimensional perspective for analysing and designing national certification systems under the European Digital Identity Wallet (EUDIW) initiative.

Williamson's model brings attention to the temporal and hierarchical structure of institutions, clarifying how societal norms, formal regulations, governance routines and technical activities are interdependent and evolve at different paces. These four layers

structure the EUDIW governance environment as follows: At the highest level, informal institutions (Layer 4), such as public trust, digital culture and user acceptance, influence the legitimacy and societal adoption of EUDIW solutions over the long term. Formal rules and legal mandates (Layer 3), shaped by EU regulations like eIDAS 2.0 and national laws, provide the institutional environment that structures compliance and governance roles. Within Layer 2, process design and institutional awareness focus on operational governance aspects, such as audit procedures, stakeholder coordination, and mechanisms for policy feedback and certification management. Finally, Layer 1 captures the technological design of the system, encompassing wallet architecture, standards, and authentication protocols that implement the foundational infrastructure and ensure technical compliance.

Koppenjan and Groenewegen's framework, in turn, provides a governance-oriented design perspective focused on how actors organize, how systems are technically structured and how processes are managed and adapted over time.

This combination ensures that both institutional depth and governance flexibility are accounted for. It helps to understand how broad EU-level mandates, like those found in eIDAS 2.0, are interpreted and implemented through practical, local-level actions within member states. The layered structure clarifies the need for legal and normative alignment, while the governance design lens emphasizes stakeholder engagement, adaptive procedures and technological interoperability.

The decision to adopt these two frameworks, rather than alternatives such as actor-network theory or multi-level governance, stems from their unique ability to combine macro-institutional analysis with actionable governance design. Williamson contributes a foundational understanding of how institutions evolve and embed over time, while Koppenjan and Groenewegen complement this with a practical lens for coordinating stakeholders and shaping responsive systems in complex, cross-border settings like EUDIW.

The resulting integrated framework supports the development of certification approaches that are context-sensitive, scalable and robust. It helps policymakers and implementers diagnose structural misalignments, coordinate design efforts and sustain trust and

functionality across legal, institutional, and technical domains. While this combined framework is well-suited for analysing complex, multi-level governance challenges like EUDIW, it may be less responsive to rapidly emerging technologies or disruptive shifts that fall outside existing institutional patterns.

Figure 4 combines both frameworks, demonstrating how EUDIW certification governance covers institutional norms, regulatory structures, decision-making routines, and technical implementations.

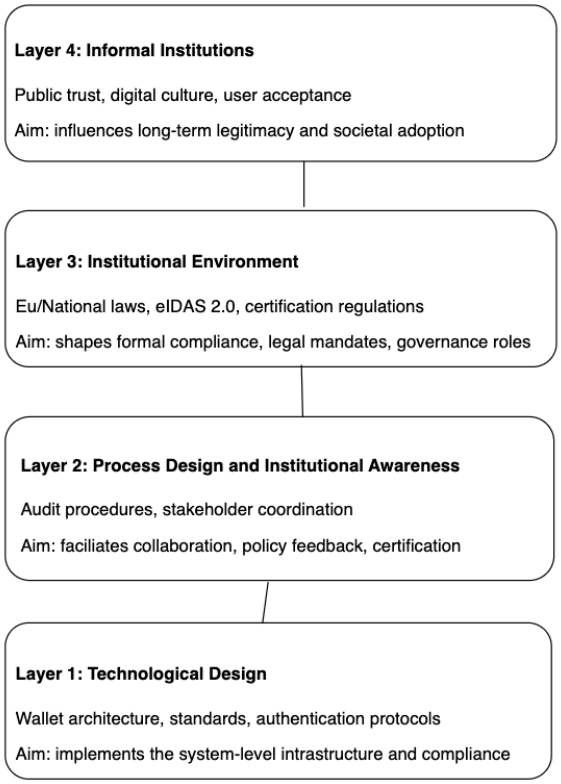

Figure 4. Institutional Governance Model for EUDIW Certification combined layers

Source: Koppenjan & Groenewegen (2005); Williamson (1998)

5 Research methodology

This chapter outlines the research design and methodology employed in this study. It explains the selected approach for examining how to develop a national certification framework for the European Digital Identity Wallet (EUDIW). The chapter details the research strategy, data collection methods and analytical techniques used to address the research questions and support the development of a preliminary certification framework.

5.1 Research strategy

This study employs a qualitative case study strategy to explore how a national certification scheme for the European Digital Identity Wallet (EUDIW) can be developed. A case study approach is particularly appropriate for this topic, as it allows for an in-depth investigation of a complex, emerging subject within its real-life context. The national-level implementation of EUDIW involves multiple interdependent factors such as technical, legal, institutional and policy-related, that cannot be fully understood through isolated or linear analysis (Gerring, 2004; Yin, 2018).

The research is framed within the broader context of European Union digital identity policy, with a specific focus on how member states, particularly Estonia, can adapt and prepare their national frameworks to support EUDIW certification Estonia serves as a relevant case due to its mature digital identity infrastructure and active participation in European eID initiatives, offering valuable insights into certification challenges and opportunities.

The research process structured around three main stages. It began with the development of a theoretical foundation to understand the relevant certification and governance concepts. This was followed by mapping the national and EU-level context, including current practices, frameworks and regulatory developments. Finally, the study conducted a comparative assessment of approaches and expert perspectives to guide the design of a certification model. The outcome of this processed sequence is a set of recommendations

and guidelines for shaping a certification framework that balances contextual needs with broader EU policy objectives. Figure 5 brings all of this together, showing how the study moved from theory and context mapping to expert input, and how those steps led to the final conclusions and recommendations.

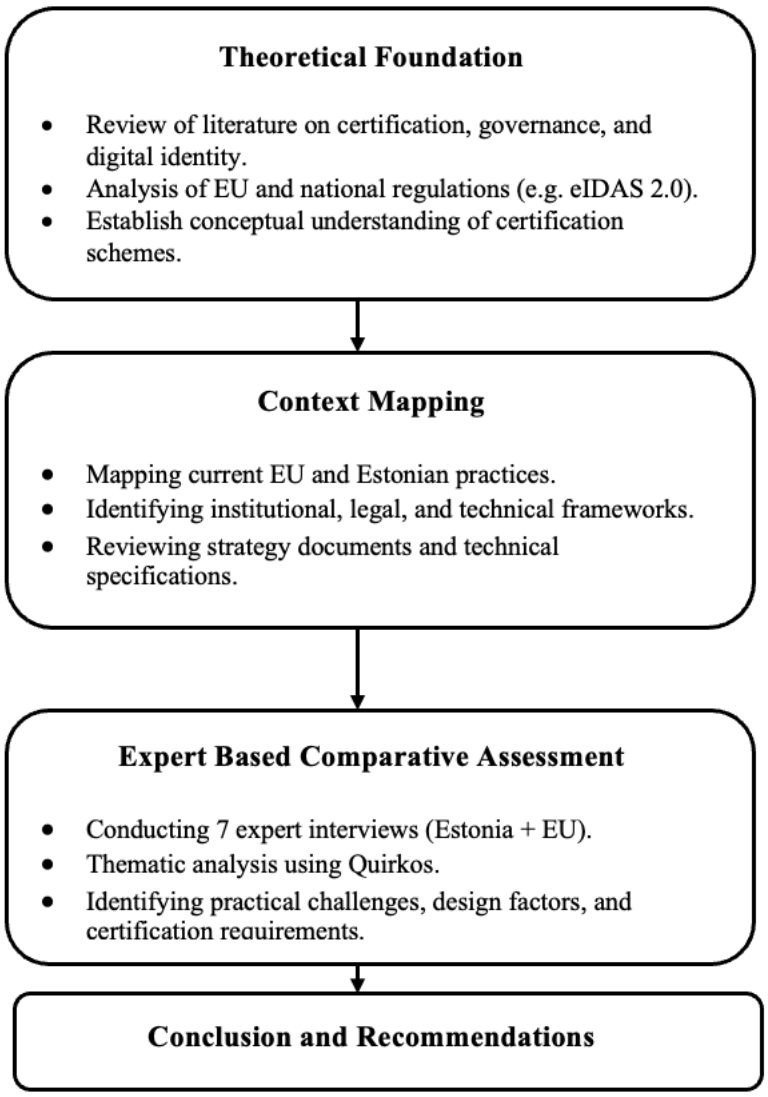

Figure 5. Outline of the research process.

Although the study followed a planned structure, the approach remained open to refinement throughout the process. Emerging regulatory updates and insights from expert interviews were integrated into the analysis where relevant. This allowed the research to stay responsive to a shifting policy landscape while maintaining a clear focus on the core objective: shaping a practical and forward-compatible national certification framework for the EUDIW.

5.2 Data collection

To support the case study approach, this research relied on multiple types of data to capture both the national and EU-level context surrounding EUDIW certification (Yin, 2018). This study utilized a combination of both primary and secondary sources, as illustrated in Figure 6.

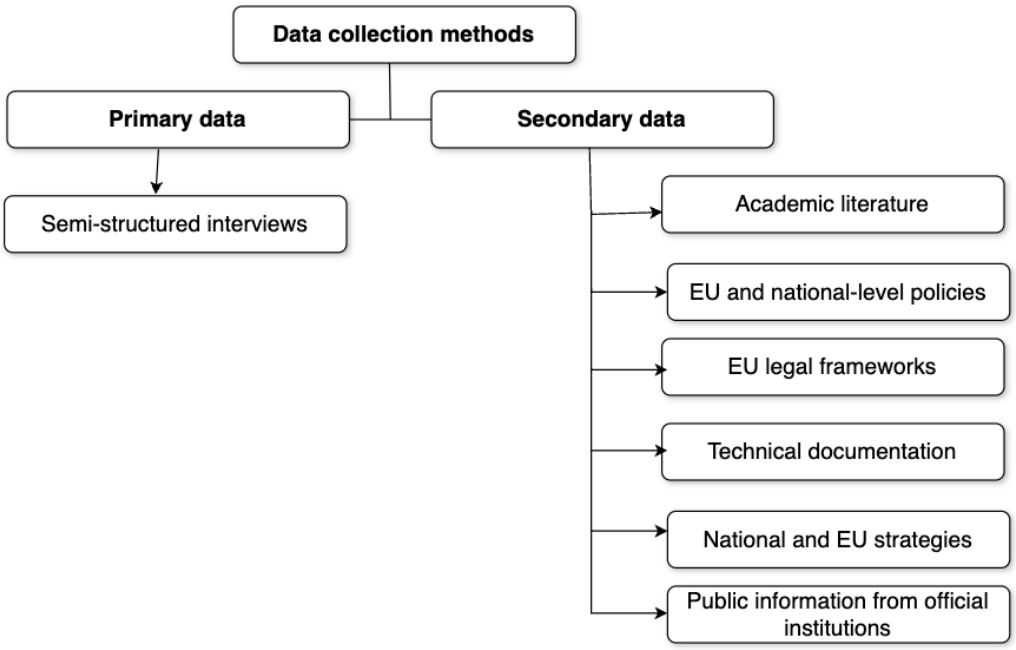

Figure 6. Primary and secondary data used for data collection.

The initial phase involved reviewing secondary data, including academic literature, legal and regulatory texts (notably eIDAS 2.0), national and EU-level policy documents, technical specifications and official strategy papers. These documents helped map the evolving institutional, legal, and technical environment relevant to EUDIW certification.

Primary data was gathered through semi-structured interviews with seven experts from Estonia and other EU countries. These individuals were selected through purposive sampling, a technique commonly used in qualitative research to identify individuals with in-depth, specialised knowledge of the subject (Patton, 2015; Etikan, 2016). Participants were chosen based on their professional experience in policymaking, certification, and digital identity management, ensuring that the data collected reflected both practical insight and subject-matter expertise. A single set of interview questions, aligned with the

research objectives, was used for all participants. The complete list of questions is available in English in Appendix 1.

To gain insight from both public and private perspectives, interviews were conducted with individuals directly involved in digital identity policymaking, implementation, or infrastructure. One interviewee represented an EU-level institution, offering a broader regulatory view, while the remaining participants were based in Estonia and selected for their practical involvement in national planning and system development related to the European Digital Identity Wallet (EUDIW).

The interviews were conducted virtually via Microsoft Teams, in either Estonian or English, and were recorded with the participants' consent. All recordings were transcribed, resulting in approximately 100 pages of source material for qualitative analysis. An overview of the interviewees, including their affiliations, roles and interview details, is presented in Table 2.

Table 2. Overview of the interviewees: affiliations, roles and interview details

Organisation's Name	**Job Title**	**Interview Format and Duration**	**Date**
SpearIT InfoSec & Compliance	Cyber Security & Electronic Trust Services Consultant, Co-Founder	Microsoft Teams Recording (38 minutes)	10.12.2024
Zetes Estonia	Country Manager in Estonia	Microsoft Teams Recording (27 minutes)	06.01.2025
KPMG	Cybersecurity Advisor and Auditor	Microsoft Teams Recording (42 minutes)	09.01.2025
Estonian Information System Authority	Chief Expert of Cyber Security Branch	Microsoft Teams Recording (45 minutes)	14.01.2025
Estonian Information System Authority	eID Competence Division Security Architect	Microsoft Teams Recording (25 minutes)	29.01.2025
Republic of Estonia Ministry of Justice and Digital Affairs	Chief Digital Identity Officer	Microsoft Teams Recording (37 minutes)	19.02.2025
Estonian Information System Authority	eID Competence Division Architect	Microsoft Teams Recording (34 minutes)	04.03.2025

5.3 Data analysis

The data analysis focused on three core themes: (1) understanding current assessment practices, (2) identifying certification requirements for the EUDI Wallet and (3) exploring the challenges and design considerations involved in shaping a national certification framework.

Interview transcripts were analysed using thematic coding with the qualitative data analysis software Quirkos (Quirkos, 2022). While the initial coding structure followed the interview questions, the process remained flexible to allow new insights to emerge during analysis. This approach ensured that both deductive and inductive themes could be captured.

Key analytical categories that emerged included certification scheme design, regulatory alignment with EU-level requirements, implementation barriers and national–EU interoperability. Thematic analysis allowed for the systematic organisation of interview data, revealing recurring patterns, areas of divergence and context-specific insights that might otherwise remain implicit.

This analytical method ensured that the findings remained grounded in expert perspectives while also surfacing critical policy and operational factors. The results of this analysis are presented in detail in Chapter 6.

6 Research results

This chapter presents the research results derived from the expert interviews conducted as part of the study. The findings are structured thematically to reflect the key areas relevant to developing a national certification framework for the European Digital Identity Wallet (EUDIW), with a particular focus on Estonia. The thematic structure was developed based on the research questions and the main governance, institutional and technical concerns that emerged during data analysis.

The results are organised into five interconnected themes. First, the chapter explores the EU-level implementation and strategic outlook to contextualise how the EUDIW initiative is unfolding at the European level. This is followed by a discussion of the key challenges in developing a national certification scheme, highlighting practical and institutional barriers identified by interviewees. The third theme focuses on Estonia's current state and progress in implementing the EUDIW, providing a snapshot of national readiness. Next, the alignment between existing electronic identification (eID) assessment practices and the new EUDIW certification requirements is analysed to identify gaps and overlaps. Finally, the chapter examines the roles and readiness of conformity assessment bodies (CABs) and the broader audit ecosystem, which are crucial for the practical rollout of certification.

This thematic grouping allows the results to be presented in a way that captures both the vertical alignment between EU and national levels and the horizontal issues across governance, legal and technical dimensions. Each section synthesises expert insights and connects them to Estonia's specific implementation context as well as broader EU coordination efforts.

6.1 EUDI Wallet's implementation in the EU

The implementation of the European Digital Identity Wallet (EUDIW) across the EU is characterized by a complex and ongoing development process. While the legislative

foundation has been laid through eIDAS 2.0, the actual operational and certification frameworks remain under construction. Experts agreed that although the goals of the initiative are shared, its practical realization is still uncertain. According to one interviewee, the EUDIW represents a shift from service-oriented audits to product certification: "*It's the first time that we're not certifying a management system or a service, but an actual product*". This shift is substantial and affects not only the scope of what must be certified, but also the methods and frequency of certification.

While ENISA has taken a central role in guiding the process, its influence is described as advisory rather than regulatory. One expert expressed skepticism about the agency's real capacity to lead, stating that "*ENISA is made up of national experts, they aren't superhuman. Real innovation still comes from countries like Austria or Belgium*". This perspective underscores the decentralized nature of implementation and the fact that meaningful progress relies heavily on national capabilities and coordination.

The EU's digital ambition, set out in the Digital Decade strategy, includes making the EUDIW a cornerstone of European identity infrastructure. However, interviews revealed that such ambitions face obstacles when filtered through national administrative structures, underfunded supervisory bodies and diverging political priorities. Although the European Commission has initiated technical working groups and stakeholder consultations, the lack of finalized standards and certification logic has led some countries to begin working on national-level solutions. There is a concern that waiting for a fully harmonized EU-wide approach may delay implementation beyond feasible timelines. As noted in multiple interviews, larger or more proactive countries may eventually create de facto standards simply by moving ahead first, which risks undermining harmonization altogether.

The very concept of certifying a product that evolves constantly through software updates is novel and challenging in the EU regulatory context. Current certification schemes are not designed to keep up with software development cycles. This is especially relevant in the EUDIW context where security patches and new functionalities must be released frequently. Without a tailored approach, certification may become either a bottleneck or a formality, compromising its trust-building purpose.

6.2 Challenges in developing a national certification scheme

Experts highlighted multiple challenges in developing a national certification scheme. These include institutional fragmentation, lack of skilled personnel, timing pressures, unclear legislative pathways and the difficulty of certifying agile products.

First, **institutional fragmentation** is seen as a key problem. In Estonia, it remains unclear which institution is ultimately responsible for coordinating and executing the certification framework. The roles of RIA, the Ministry of Justice and Digital Affairs and third-party auditors are all relevant, but coordination among them is insufficient. This fragmentation also emerged in expert interviews as a broader European challenge: digital identity management spans cybersecurity, public administration and data protection, yet no single agency appears to hold comprehensive oversight across these domains.

Another major challenge is the **lack of skilled personnel**. Estonia currently lacks auditors who are trained to evaluate cybersecurity or digital wallet products. As one expert put it, "*Even if we have a scheme, there are no auditors to do it. Who certifies the app? Who checks the backend"*. This skill gap extends beyond auditors to scheme designers and policymakers and creates a bottleneck in readiness. The absence of an accredited cybersecurity certification ecosystem means that even the most basic prerequisites for running a national scheme are missing.

Timing is another critical issue. The legal deadlines set at the EU level are described as misaligned with national capabilities. One interviewee estimated that it would take approximately 1.5 years to design, implement and test a functioning certification scheme in Estonia. However, the regulation expects readiness in less time. This creates pressure to deliver prematurely or to rely on interim solutions with questionable robustness.

In addition, the **lack of a defined legislative pathway** has resulted in policy uncertainty. There is still no domestic regulation or guidance that would allow Estonia to establish a scheme that aligns with eIDAS 2.0 and the anticipated ENISA cybersecurity scheme. According to one expert, "*Estonia lacks a legal roadmap for becoming an E-ITS auditor, let alone EUDIW ones*".

Finally, **technical certification schemes** in use today are generally not built for agile, frequently updated products like the EUDI Wallet. One expert described the challenge as follows: "*The challenge is to certify something agile. But certification frameworks are designed for stability, not flexibility*". This is compounded by the need to coordinate various assurance layers, functionality, cryptographic robustness and user experience, within one framework.

These national-level challenges, ranging from fragmented institutional roles to skill shortages are particularly relevant when considering Estonia's own readiness to implement EUDIW. The following section zooms in on Estonia's context, highlighting both its strengths and the specific gaps it must address.

6.3 Estonian EUDIW implementation

Although Estonia is widely regarded as a leader in digital governance, its preparedness to implement the EUDIW is mixed. According to several interviewees, Estonia's current eID infrastructure is advanced but not aligned with the requirements of EUDIW. It is primarily based on static PKI infrastructure and hardware tokens rather than mobile-first identity platforms. As a result, adaptation would require building a parallel system from scratch. One expert remarked that "*Estonia's current EID schemes cannot simply be upgraded, they must evolve into a new ecosystem*".

Experts stressed that Estonia should not delay beginning the design of its national certification scheme. Waiting for a fully developed EU framework could result in missed opportunities and delayed readiness. One expert advised that Estonia should "*start national scheme prototyping early, don't wait for EU-level harmonization*". Collaboration with neighbouring countries, particularly Finland and other Baltic states, was also recommended to accelerate mutual learning and reduce duplication of effort.

Leadership and coordination issues also persist. According to one interviewee, responsibility is split across various government bodies and there is no clear chain of command. This fragmentation risks impeding both the planning and execution of the certification scheme. The current governance model is not optimized for the cross-sectoral nature of the wallet, which touches public sector infrastructure, private sector implementation and end-user adoption.

Another issue raised was the limited role of citizen engagement. Although the EUDIW is ultimately intended to serve the public, few mechanisms currently exist for citizen input. One expert proposed facilitated workshops to allow citizens to understand the wallet and raise concerns, especially around data control and inclusion.

6.4 Alignment between eID schemes assessment and EUDIW certification requirements

While the EUDIW initiative builds on eIDAS principles, the interviewees unanimously agreed that the alignment between current eID schemes assessment and EUDIW certification requirements is limited. Several experts pointed out that although both systems aim to ensure trust and security, the methods and contexts differ substantially.

For instance, traditional eID schemes typically involve certifying backend systems and processes, whereas EUDIW focuses on certifying a mobile application as a product. One expert explained, "*We are now talking about something completely new, new structures, content types, and even new expectations about what identity means*".

Some areas of partial alignment were acknowledged, particularly in cross-border authentication and qualified signatures. As another expert noted, "*The closest where alignment may happen is regarding authentication and the cross-border part*".

However, fundamental changes in how identity data is structured and managed, particularly with the introduction of Electronic Attestation of Attributes (EAA), represent a significant departure from practices established under the original eIDAS Regulation (*Regulation (EU) No 910/*2014, 2014), which many national systems still follow. Existing risk assessment models are also insufficient, as they do not account for the new threat landscape introduced by mobile-first architecture and decentralized identity components. Experts observed that existing eID systems often rely on fixed data structures and that transitioning to attribute-based attestations requires a deep overhaul of technical and legal processes. As of spring 2025, a revised version of the EAA Implementing Act remains under discussion in the European Commission's comitology process coordinated with the eIDAS Expert Group, and its adoption has been delayed by over five months.

Moreover, conformity assessment bodies accustomed to auditing centralized architectures will have to develop new methodologies for evaluating distributed, user-controlled wallets. These methodological gaps are compounded by the lack of sector-specific guidance or standardized testing protocols at the EU level.

While the overall alignment between current eID scheme assessments and EUDIW certification requirements is limited, interviewees identified several areas where some continuity exists. Most notably, cross-border authentication remains a shared objective, with both frameworks aiming to ensure seamless identity verification across EU member states. Similarly, qualified electronic signatures continue to play a critical role, providing legal certainty and interoperability under both systems. Some experts also pointed to trust list interoperability and the use of qualified trust service providers (QTSPs) as examples of elements that carry over from eIDAS 1.0. In addition, the notification procedures for national eID schemes, a regulatory feature under eIDAS are expected to remain relevant in the broader EUDIW governance structure. These partial alignments, while not sufficient to bridge the full methodological gap, may provide useful starting points for designing a more integrated and future-proof certification model.

6.5 Key technology and regulatory alignment

One of the core findings from the interviews is the misalignment between current technological capabilities and the regulatory expectations of EUDIW implementation. Several experts emphasized the importance of developing a hybrid certification model. Such a model would include static certification for cryptographic hardware and flexible, dynamic certification for mobile app components. This approach was seen as essential given the constant updates and patches that mobile applications require.

Many interviewees also expressed concern over the maturity of the technical standards being proposed. Specific issues were raised about cryptographic module specifications and privacy-preserving technologies. One expert observed that key technologies such as zero-knowledge proofs were not yet mandated, even though they could address many privacy concerns inherent in the EAA system. The result is a certification scheme that risks enshrining outdated security models unless continuously revised.

ENISA's role in the regulatory alignment process was frequently described as limited. Although ENISA provides valuable guidance, it does not have the mandate or authority to enforce standards. As one expert noted, "*ENISA is a distribution agency. They give only guidance, not concrete rules"*.

Furthermore, participants emphasized the need to draw inspiration from other regulatory ecosystems. The U.S. system was mentioned as an example, particularly for its modular, pluggable certification logic. This flexibility was contrasted with the rigidity of current EU approaches. It was argued that a modular model would better support the fast-paced development cycles of modern digital identity products. Such a framework would allow parts of the wallet to be re-certified independently, without invalidating the entire application.

Finally, the social and ethical dimensions of digital identity systems were said to be underrepresented in the design of EUDIW. As one interviewee pointed out, current discussions focus heavily on business value and technical functionality, but neglect issues such as privacy, non-discrimination and user agency. Without incorporating these concerns, there is a risk that the wallet will be technically secure but socially untrusted. For a system intended to be used daily by millions of European citizens, trust must be earned not only through encryption, but through transparency, inclusion and accountability.

6.6 Role of Conformity Assessment Bodies and auditors

Several interviewees emphasized that one of the most under-discussed yet critical components of the EUDIW certification ecosystem is the readiness and capacity of conformity assessment bodies. In the current context, these bodies are expected to bridge the gap between legal requirements, technical standards and practical auditing capacity. Yet most national ecosystems, including Estonia's, lack accredited organizations that could conduct a full-scope EUDIW certification audit.

One interviewee pointed out that the EU is relying on a small pool of experts who already struggle to maintain continuity in existing eIDAS audits. Transitioning to a product-based certification system for wallets, which requires competence in software development, cryptographic engineering, mobile security and privacy law, raises the bar considerably.

According to this expert, "*Even the largest CABs are not prepared. There is no shared methodology, no auditor training program, and no cross-border recognition yet."*

Additionally, a structural issue was raised regarding the lack of separation between scheme ownership and certification responsibility. Without clear independence between those who build the wallet and those who audit it, the credibility of the certification process may be at risk. The same expert also noted that Estonia's current legal structure does not provide sufficient room for private-sector conformity assessment bodies to emerge, further limiting innovation.

Some interviewees did highlight encouraging examples, particularly Belgium's proactive role in wallet prototyping and Germany's investment in auditor capacity building. Estonia was also mentioned as having early discussions on involving universities in future auditor training, though concrete initiatives remain limited.

In terms of solutions, interviewees recommended the creation of a pan-European training network for auditors, potentially hosted or coordinated by ENISA. Furthermore, it was suggested that auditing frameworks could adopt modular logic, allowing assessors to specialize in specific components of the wallet such as backend APIs, secure hardware environments, or user interface layers. This would not only reduce the cognitive burden on auditors but also encourage collaboration among CABs.

Finally, concerns were raised about liability. If a wallet is certified and later found to have vulnerabilities, it is unclear who bears responsibility, the certifier, the scheme owner, or the regulator. The lack of clarity here may deter organizations from stepping into the auditor role at all.

These concerns underscore the fact that no certification scheme can succeed without a strong and credible auditing infrastructure. For any member state aiming to lead in EUDIW implementation, establishing this ecosystem, complete with trained auditors, clear governance structures, and liability frameworks, is not just important, but urgent. Without it, the credibility and functionality of the entire certification process remain at risk.

7 Discussion

This chapter interprets the empirical findings of the thesis and positions them in relation to the broader context of digital identity governance within the European Union. It builds on the research goal of understanding how a national certification scheme for the European Digital Identity Wallet (EUDIW) can be shaped, focusing on Estonia's role and readiness. While Estonia is often regarded as a frontrunner in digital service provision, this study reveals that institutional maturity alone does not guarantee certification readiness. Instead, multi-level challenges, legal, technical and organisational, must be addressed to align with eIDAS 2.0 objectives.

One of the key takeaways is that the certification of a dynamic, user-facing digital wallet differs substantially from traditional certification approaches used for backend identity systems. The mobile-first, privacy-centric and cross-border nature of the EUDIW introduces a new layer of complexity. Certification must now encompass not only infrastructure-level security and regulatory compliance but also usability, privacy-enhancing technologies and ongoing software maintenance. This shift reflects a deeper transformation in the object of certification, from static, infrastructure-based systems to agile, modular applications, which existing conformity assessment models are not well equipped to handle.

From an institutional perspective, this misalignment highlights challenges between regulatory ambition (Layer 3) and technical implementation (Layer 1), as conceptualised by Williamson's four-layer model. A static certification approach is not sufficient for an evolving ecosystem, yet current risk assessment methodologies are not designed for iterative development or continuous deployment.

Institutionally, the analysis highlights fragmentation in Estonia's governance landscape. There is currently no clear lead agency responsible for coordinating wallet certification activities. The roles of the Estonian Information System Authority (RIA), the Ministry of Justice and Digital Affairs and the national accreditation body are not sufficiently delineated. This poses challenges for accountability, especially in the context of cross-

border recognition and legal liability. The governance design perspective by Koppenjan and Groenewegen further underscores this gap, Estonia's certification ecosystem lacks clearly defined roles, interdependencies and coordination mechanisms needed for effective implementation.

Furthermore, Estonia lacks accredited conformity assessment bodies (CABs) that can certify the wallet's functionalities, posing a risk to timely implementation. This capability gap is especially problematic given the tight timelines imposed by EU-level regulation and the requirement for cross-border mutual recognition of certification outcomes.

The study also points to the critical role of the European Commission and ENISA in developing overarching certification guidelines. However, the operational burden will rest with individual member states. In this context, national frameworks must remain aligned with EU-level objectives while retaining enough flexibility to adapt to local legal, technical and infrastructural specificities. At the same time, delays in the adoption of several relevant implementing acts reflect broader timing misalignments between EU-level rule-making and national implementation planning.

Although the sample included one EU-level expert from the trust services domain, the absence of interviewees from the European Commission and ENISA is a limitation. In addition, the study did not include voices from civil society, developers involved in EUDI Wallet pilot projects, or end-users. These perspectives could have added valuable insight into citizen expectations, ethical considerations and the practical implications of certification from a non-institutional viewpoint.

Moreover, the research reveals the importance of public trust and inclusive design in the context of EUDIW certification. Technical robustness alone is not sufficient, citizen engagement, transparency in certification criteria and user testing are equally vital. Certification should therefore be understood not only as a regulatory or security instrument but also as a societal trust mechanism. This reframing positions certification as a tool that supports democratic values and fosters legitimacy.

The need for modularity, governance clarity and capacity building emerged as recurring themes during expert interviews. These findings suggest that Estonia, and other member states, must not only meet formal regulatory requirements but also invest in institutional and technical readiness to operationalise certification schemes. A successful approach

requires coordination across regulatory, governance, and infrastructural layers, as well as collaboration between public authorities, auditors, developers, and end-users.

In conclusion, while Estonia possesses many foundational elements needed for EUDIW certification, it must address institutional fragmentation, close capability gaps and develop governance arrangements that are both agile and transparent. These insights also provide a foundation for practical responses, which are further developed in the recommendations and the conceptual framework presented in the following chapters. While some methodological constraints and gaps were acknowledged in the discussion above, a more systematic overview of the study's limitations and future research directions is provided in Chapter 9.

7.1 Recommendations

Based on the findings, the following recommendations are proposed to guide Estonia and other EU member states in developing effective EUDIW certification schemes:

- Establish clear national governance structures. Define a lead agency with legal authority and coordination capacity. In Estonia, this could involve clarifying the roles between RIA, the Ministry of Justice and Digital Affairs and the national accreditation body.
- Create a modular certification framework. A flexible approach combining static assessments (e.g. infrastructure security) with dynamic ones (e.g. updates to mobile apps) is crucial. Certification criteria should include user interface usability, cryptographic robustness, compliance with GDPR and interoperability with existing eID and SDG infrastructures.
- Prioritize CAB readiness. Estonia currently lacks accredited bodies with the skills to audit EUDIW. It is vital to invest in auditor training programs, potentially co-developed with ENISA and regional partners such as Finland.
- Launch a reference prototype. Develop a national reference implementation of the wallet to facilitate testing and certification trial runs. This can help simulate real-world conditions and identify gaps in requirements.

- Align certification processes with EU standards. Active participation in EU technical working groups and bilateral pilots (e.g. NOBID) will help ensure that Estonia's certification logic remains compatible and contributes to mutual recognition.
- Address liability frameworks. Clarify who holds responsibility in case a certified wallet fails, whether it is the CAB, scheme owner, or regulator. Legal clarity is necessary to incentivize market participation.
- Engage the public. Promote transparency by involving citizens in user testing and feedback loops. This helps ensure the wallet is inclusive and builds trust.
- Integrate socio-ethical standards. Certification should also consider accessibility, digital inclusion, and non-discrimination. This ensures alignment with EU values and fosters broader public legitimacy

8 Conceptual framework for EUDIW certification

This chapter presents the author's original contribution to the thesis, a conceptual framework designed to support the development of a national certification scheme for the European Digital Identity Wallet (EUDIW). The framework is the result of an interpretive synthesis that combines the empirical insights gathered from expert interviews, the theoretical models introduced earlier, and the context-specific challenges identified in Estonia. It bridges theoretical understanding and empirical evidence through a tool that is both strategic and practically applicable.

The author's contribution lies in translating complex, multi-level challenges into a structured and actionable roadmap for national implementation. While the European Commission and ENISA provide strategic direction and regulatory guidance, national-level implementation remains fragmented and uneven. This framework aims to bridge that gap by offering a modular, governance-sensitive tool that enables policymakers, public sector leaders and conformity assessment bodies to structure their actions, responsibilities, and timing. The value of this contribution lies in three core aspects: it offers a structured lens to diagnose and prioritise challenges, delivers a concrete yet adaptable tool under uncertainty and serves as a replicable model for other digitally advanced member states.

The framework consists of two complementary tools that together form a robust and adaptable structure. The first is a domain-based matrix that identifies key readiness areas, the actors involved, and the corresponding actions required. The second is a practical implementation checklist that breaks these domains into concrete, sequenced steps. Together, these tools support both high-level planning and day-to-day execution. Its robustness is grounded in conceptual clarity, empirical foundation and real-world applicability, designed with Estonia in mind, but scalable across the EU.

8.1 Key domains for EUDIW implementation

The first part of the framework is a domain-based matrix (Table 3). It outlines eight strategic domains that emerged during the analysis as central to successful certification: governance, legal clarity, audit ecosystem, technical design, assurance layering, stakeholder alignment, interoperability and citizen trust. For each domain, the matrix identifies the main challenge, responsible actors and key recommended actions.

This domain-based model reflects the core insight that EUDIW certification is not just a technical task, but a systemic coordination challenge. It supports structured planning, helps identify gaps in role ownership and provides a shared vocabulary for inter-agency dialogue. It also serves as a conceptual diagnostic tool for policymakers seeking to prioritise actions across multiple, interdependent readiness areas.

Table 3. Key domains and actions for EUDIW implementation
Source: Synthesized from Chapters 5.1-5.3 and 6.2–6.6

Domain	**What to address**	**Key actors**	**Recommended action**
Governance & coordination	Clear roles and responsibilities across government bodies	Ministries, digital agencies	Designate a lead agency and form an interagency task force
Certification scheme design	National certification aligned with EU-level rules	Supervisory authorities, ENISA, CABs	Start early prototyping; consider hybrid (static + dynamic) models
Legal & regulatory framework	Domestic laws supporting scheme ownership, audit roles, liability	Legislators, legal experts	Develop EUDIW-compatible laws and ensure independence of auditors
Auditor ecosystem	Skilled assessors, independence, training	CABs, ENISA, universities	Launch national training programs and promote modular specialization
Technical standards & tools	EAA support, cryptography, privacy-by-design, modular testing	Tech experts, wallet developers	Adopt modern standards (e.g., ISOs); ensure modularity and frequent update capability
Infrastructure readiness	Mobile-first architecture, parallel eID systems	Government IT teams, private providers	Develop mobile-first wallet infra; don't rely on outdated PKI alone
EU alignment & cooperation	Compatibility with EU specs, mutual recognition	National authorities, EU bodies	Join EU working groups; seek early peer alignment with other member states
Public engagement & trust	Transparency, citizen participation, inclusion	Civil society, UX Teams	Run citizen workshops; communicate use, rights, and data handling clearly

8.2 Practical implementation checklist

The second part of the framework is a practical checklist (Table 4) that translates the domains above into sequenced, actionable steps. The checklist serves as a tool for implementation teams within government ministries, accreditation authorities and associated institutions. It can be used to structure task forces, set deadlines, and monitor progress.

The eight steps are grouped by function: steps 1–2 establish governance arrangements and prototyping capacity; steps 3–4 address legal mandates and audit readiness; steps 5–6 support wallet-level implementation and assurance mechanisms; and steps 7–8 align the national scheme with EU actors and citizen expectations.

Table 4. EUDIW implementation checklist
Source: Synthesized from Chapters 5.1-5.3 and 6.2–6.6

Step	Action Area	Checklist Item
1	Governance	☐ Appoint a lead ministry or digital authority
		☐ Establish interagency coordination model
2	Certification scheme	☐ Design hybrid certification model (product + updates)
		☐ Involve ENISA guidance early on
3	Legal & regulatory framework	☐ Pass national law enabling EUDIW audits
		☐ Ensure legal separation between scheme owners and auditors
4	Auditor ecosystem	☐ Identify and accredit conformity assessment bodies (CABs)
		☐ Launch national or EU-led auditor training program
5	Technical readiness	☐ Design modular wallet architecture
		☐ Use current standards (EAA, secure modules, mobile security)
		☐ Enable regular software updates and recertification mechanisms
6	Infrastructure	☐ Build mobile-first wallet system
		☐ Avoid relying on outdated static eID infrastructure
7	EU & peer alignment	☐ Participate in EU technical and policy working groups
		☐ Align testing and certification with neighbouring countries
8	Public engagement	☐ Organize user testing and citizen consultations
		☐ Communicate wallet purpose, benefits, and data safeguards clearly

The checklist ensures that no critical dimension is left behind by aligning these steps with stakeholder responsibilities. Its adaptability allows member states to tailor it to their institutional context, maturity level and implementation timeline. Beyond execution, it supports progress monitoring and facilitates cross-border learning, making it a strategic and operational guide for national authorities navigating certification under uncertainty.

9 Limitations and future work

This chapter outlines the key limitations encountered during the development of this study and proposes directions for future research. It reflects on the specific regulatory and institutional constraints within both the Estonian and European Union contexts that shaped the research scope. Furthermore, it considers how the findings can inform broader discussions on digital identity governance and support the ongoing development of certification frameworks for the EUDIW across member states.

9.1 Limitations

While this study provides important insights into the development of a national certification framework for the EUDIW, several limitations must be acknowledged. First, the timing of the research posed a challenge. As the eIDAS 2.0 Regulation and the technical specifications for the EUDIW were still under development during this thesis, some findings may be affected by subsequent regulatory updates. The evolving nature of both the legal texts and the wallet architecture means that specific recommendations may need to be revisited.

The scope of the study is also geographically limited. Estonia was chosen as a single-country case study due to its advanced digital infrastructure and proactive role in EU digital identity initiatives. However, this choice narrows the applicability of the findings to other member states, particularly those with less mature digital identity ecosystems or different institutional arrangements.

Another limitation lies in the composition of the interview sample. The seven expert interviews included both national and EU-level perspectives, with one expert representing an EU-wide view from the trust services and cybersecurity domain. The remaining interviewees were primarily national stakeholders from Estonia, including public sector officials from the Information System Authority and the Ministry of Justice and Digital Affairs, as well as cybersecurity consultants and auditors. However, the sample did not include representatives from core EU institutions such as the European Commission or

ENISA, nor did it include developers involved in EUDI Wallet pilot projects, civil society organisations, or end-users. These actors could have offered important insights into regulatory intent, citizen expectations, and implementation realities from user-centric and ethical standpoints. A broader and more diverse sample might have contributed to a more comprehensive understanding of the certification challenges across different levels of governance and affected stakeholder groups.

Finally, the study was constrained by access to confidential or unpublished policy drafts. As several key materials, both at the national and EU level, remain restricted or are still under development, the thesis had to rely on publicly available information and indirect insights. Despite these limitations, the study presents a valuable contribution to the growing body of work on digital identity governance and offers a structured foundation for further research.

9.2 Future research directions

Building on the findings and constraints of this thesis, several future research paths are suggested. Comparative research across multiple EU member states would provide a more nuanced understanding of how national contexts influence certification readiness and institutional alignment. Such cross-country studies could help determine which governance and legal models best support the goals of EUDIW certification and how mutual recognition between schemes can be achieved.

Future work should also include technical experimentation, such as developing and evaluating reference implementations of EUDIW wallets. Prototyping efforts could simulate real-world usage and certification assessments, generating empirical data to refine security criteria, usability standards, and testing protocols. In addition, future research should examine how the proposed framework could be applied in practice, specifically, how the actual development of a national certification scheme unfolds when guided by this model and what adaptations may be necessary in real-world settings.

Further investigation into the end-user perspective is also needed. Public trust, perception of certification labels and concerns about data protection must be explored through qualitative studies such as focus groups or quantitative surveys. Understanding how users

engage with certified wallets will ensure that certification frameworks are not only technically sound but also socially accepted.

In addition, long-term evaluations of certification impact could be conducted. These would assess the effectiveness and durability of certified wallets in practice, including their performance during incidents, their resilience to regulatory changes, and their contribution to service reliability and trust.

Finally, future research should delve into the economic dimension of certification. This includes analysing the cost structures and revenue models for conformity assessment bodies, exploring incentives for wallet developers and issuers and assessing the potential market implications of mandatory certification. Additionally, a forward-looking perspective should consider whether it is more cost-effective and strategically beneficial for a member state to develop its own national certification scheme or to join a broader cross-border initiative, such as the NOBID or Benelux model, coordinated by multiple EU countries.

10 Summary

This thesis set out to examine how a national certification scheme for the European Digital Identity Wallet (EUDIW) could be developed, using Estonia as a case study. Drawing on theoretical models, expert interviews and regulatory analysis, the research investigated the challenges, opportunities and strategic requirements associated with wallet certification in the context of eIDAS 2.0.

The findings demonstrate that while Estonia possesses a strong digital infrastructure, its readiness for EUDIW certification is limited by institutional fragmentation, the absence of specialized CABs and uncertainties regarding governance roles. These gaps are compounded by the innovative nature of the wallet, which departs significantly from existing eID paradigms and introduces new requirements in usability, security and data protection.

To address these issues, the thesis proposes a conceptual framework that synthesises empirical findings and institutional theory into a structured roadmap for national EUDIW certification**.** This approach emphasizes national coordination, flexible technical standards and alignment with EU-level initiatives. In addition, the research offers a set of practical policy recommendations, including the development of a reference prototype, the training of auditors and the inclusion of citizens in testing and feedback processes.

Certification, in this context, must be understood as more than a regulatory mechanism, it functions as a trust-enabling process that integrates legal, technical and societal dimensions. For the EUDIW to succeed at both national and EU levels, certification must be treated not only as a compliance requirement but as a driver of legitimacy, usability and public confidence**.** The work laid out in this thesis provides a conceptual foundation and practical contribution for such a certification framework and invites further inquiry as Europe moves toward full-scale implementation of its digital identity vision.

In conclusion, this thesis answered its main research question and sub-questions by offering both theoretical insights and practical tools to guide national EUDIW certification efforts. The proposed framework contributes to bridging current gaps and lays a foundation for further development and cross-border coordination in digital identity governance.

References

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

Andrade, F. H. (2023). *Certification Services in Face of the Portuguese DL 12/2021*. Social Science Research Network. https://doi.org/10.2139/ssrn.4519844

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

Busch, C. (2022). *eIDAS 2.0: Digital identity services in the platform economy*. Centre on Regulation in Europe (CERRE). https://cerre.eu/publications/eidas-2-0-digital-identity-services-in-the-platformeconomy/

Council of the European Union. (n.d.). *A digital future for Europe*. https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/

Cuijpers, C., & Schroers, J. (2014). eIDAS as a guideline for the development of a pan-European eID framework in FutureID.

Cybernetica. (2023). *Digikukru I etapi analüüs*. Prepared for the Information System Authority (RIA). https://www.ria.ee/riigiinfosusteem/elektrooniline-identiteet-ja-usaldusteenused/digikukkur-eesti-wallet

Czerny, R., Kollmann, C., Podgorelec, B., Prünster, B., & Zefferer, T. (2023). Towards a Mobile-First Cross-Border eID Framework. In 24th Annual International Conference on Digital Government Research - Together in the unstable world: Digital government and solidarity (DGO 2023), July 11–14, 2023, Gdańsk, Poland. ACM, New York, NY, USA, 10 pages.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Doshi, A. R., & Schmidt, W. (2024). Soft Governance Across Digital Platforms Using Transparency. *Strategy Science*, 9(2), 185–204

e-Estonia. (2024). *E-Services & registries – e-Estonia*. https://e-estonia.com/solutions/e governance/e-services-registries/

ENISA. (2023). *Digital Identity Standards*. https://www.enisa.europa.eu/publications/digital-identity-standards

Etikan, I. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1–4. https://www.researchgate.net/publication/304339244_Comparison_of_Co venience_Sampling_and_Purposive_Sampling

European Commission (2021). Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust. https://eur-lex.europa.eu/legal

content/EN/TXT/?uri=celex:52021DC0290
European Commission. (2023). The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework. https://www.intesigroup.com/en/wp-content/uploads/sites/4/2023/02/ARF-v1.0.0-final.pdf
European Commission. (2014). *Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)*. Official Journal of the European Union. https://eur-lex.europa.eu
European Commission. (2024a). *Commission Implementing Regulation (EU) 2024/2977*. Official Journal of the European Union. https://eur lex.europa.eu/eli/reg_impl/2024/2977/oj/eng
European Commission. (2024b). *Commission Implementing Regulation (EU) 2024/2979*. Official Journal of the European Union. https://eur lex.europa.eu/eli/reg_impl/2024/2979/oj/eng
European Commission. (2024c). *Commission Implementing Regulation (EU) 2024/2980*. Official Journal of the European Union. https://eur lex.europa.eu/eli/reg_impl/2024/2980/oj/eng
European Commission. (2024d). *Commission Implementing Regulation (EU) 2024/2981*. Official Journal of the European Union. https://eur lex.europa.eu/eli/reg_impl/2024/2981/oj/eng
European Commission. (2024e). *Commission Implementing Regulation (EU) 2024/2982*. Official Journal of the European Union. https://eur lex.europa.eu/eli/reg_impl/2024/2982/oj/eng
European Commission. (2024f). *Regulation (EU) 2024/1183 establishing a framework for a European Digital Identity*. Official Journal of the European Union. https://eur lex.europa.eu/eli/reg/2024/1183/oj/eng?eliuri=eli%3Areg%3A2024%3A1183 3Aoj&locale=en
European Commission. (2024g). *European Digital Identity Wallet – Large Scale Pilots*. https://ec.europa.eu/digital-building blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+ cale+Pilot+Projects
European Commission. (2024h). *Implementing Acts for eIDAS 2.0*. https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation
European Commission. (2024i). *European Digital Identity*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
European Commission. (2024j). *European Digital Identity Architecture and Reference Framework – Outline*. https://eu-digital-identity-wallet.github.io/eudi docarchitecture-and-reference-framework/1.4.0/arf/
European Commission. (2024k). Technical Specifications—EU Digital Identity Wallet. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Technical+Specifications
European Data Protection Board. (2021). *Guidelines on certification under GDPR*. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en
European Parliament, & Council of the European Union. (2022). *Decision (EU) 2022/2481 of the European Parliament and of the Council establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance)*. *Official Journal of the European Union*, L

323, 4–26. https://eur-lex.europa.eu/eli/dec/2022/2481/oj

European Union Agency for Cybersecurity. (2024). *EU Digital Identity Wallet: A leap towards secure and trusted electronic identification through certification*. https://www.enisa.europa.eu/news/eu-digital-identity-wallet-a-leap-towards-secure-and-trusted-electronic-identification-through-certification

Fernández, R. R. (2024). *Evaluation of trust service and software product regimes for zero knowledge proof development under eIDAS 2.0*. *Computer Law & Security Review*, 53, 105968. https://www.sciencedirect.com/science/article/pii/S0267364924000359?ssrnid 4505887&dgcid=SSRN_redirect_SD

Fernández, R.R. (2023). Evaluation of Trust Service and Software Product Regimes for Zero Knowledge Proof Development Under eIDAS 2.0

Gallo, C., Giove, M., Millard, J., Kåre, R., & Thaarup, V. (2014). *Study on e-Government and the reduction of administrative burden: final report.* Publications Office. https://data.europa.eu/doi/10.2759/42896

Gerring, J. (2004). What is a case study, and what is it good for? American Political Science Review, 98(2), 341-354. https://www.researchgate.net/publication/224952190_What_is_a_Case_Study_and_ What_is_it_Good_For

Hölbl, M., Kežmah, B., & Kompara, M. (2023). eIDAS Interoperability and Cross-Border Compliance Issues. *Mathematics*, *11*(2), 430. https://doi.org/10.3390/math11020430

ITEH. (2024). *ISO/IEC 29115:2013 Authentication Assurance Framework*. https://cdn.standards.iteh.ai/samples/45138/31391aa0c87a48e192194661d81a0 bc/ISO-IEC-29115-2013.pdf

Kalvet, T., Toots, M., van Veenstra, A. F., & Krimmer, R. (2018). Cross-border e-Government Services in Europe: Expected Benefits, Barriers and Drivers of the Once Only Principle. *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, 69–72. https://doi.org/10.1145/3209415.3209458

Kawamura, A. (2023). *The European Union Electronic Identity and Data Protection in the Finnish and Estonian Legal Systems*. https://digikogu.taltech.ee/et/Item/c5ef7654-074b-47f3-bdfe-fa862df38c02

Koppenjan, J., & Groenewegen, J. (2005). Institutional design for complex technological systems. *International Journal of Technology, Policy and Management*, *5*(3), 240. https://doi.org/10.1504/IJTPM.2005.008406

Lee, Y., Kozar, K., & Larsen, K. (2003). The Technology Acceptance Model: Past, Present, and Future. *Technology*, *12*. https://doi.org/10.17705/1CAIS.01250

Maierhofer, S., & Schimpe, S. (2022). Design Principles for EU Cross-Border Services. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13391 LNCS*, 93- 105. Scopus. https://doi.org/10.1007/978-3-031-15086-9_7

Matus, K. (2009). Standardization, certification and labeling: lessons from theory and practice. https://www.researchgate.net/publication/49938713_Standardization_certification_ nd_labeling_lessons_from_theory_and_practice

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2024). A Survey on Decentralised Identifiers and Verifiable Credentials. 10.13140/RG.2.2.12726.92485.

Mocanu, S., Chiriac, A. M., Popa, C., Dobrescu, R., & Saru, D. (2019). *Identification and Trust*

Techniques Compatible with eIDAS Regulation (pp. 656–665). Springer, Cham. https://doi.org/10.1007/978-3-030-21373-2_55

Mölder, E.M. (2024) EU Cross-border Service Delivery Analysis in the Context of eIDAS 2.0. https://digikogu.taltech.ee/et/Item/ce579f71-7070-4b35-9497-9dc4dbabfc42

Morosi, M. (2022). *Study of authentication models and implementation of a prototype by using eID and Distributed Ledger Technologies.* https://webthesis.biblio.polito.it/25565/

Nakashidze, M. (2023). Democracy, Rule of Law, and Protection of Human Rights in the European Union. https://www.researchgate.net/publication/377336937_Democracy_Rule_of_Law_and_Protection_of_Human_Rights_in_the_European_Union

Nguyen, K. (2018). Certification of eIDAS trust services and new global transparency trends: Forming the basis for trust: certification and transparency. Datenschutz und Datensicherheit - DuD. 42. 424-428. https://link.springer.com/article/10.1007/s11623-018-0972-7

NIST (2024). *Cybersecurity Framework Version 2.0*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NOBID Consortium (2023). *About the NOBID Consortium*. https://www.nobidconsortium.com/about/

Õunapuu, G. (2024). *Differences in cross-border compliance for providing trust services for national electronic identity means*. https://digikogu.taltech.ee/et/Item/98faa4bd-9d99-46fd-82fb-e08923910395

Patton, M. Q. (2015). Qualitative research & evaluation methods: Integrating theory and practice (4th ed.). Sage Publications. https://tms.iau.ir/file/download/page/1635851437-michael-quinn-patton- qualitative-research-evaluation-methods-integrating.pdf

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

Poste Italiane (2024). *Poste Italiane joins the NOBID project for the European Digital Identity Wallet*. https://www.posteitaliane.it/en/nobid-project.html

Quirkos. (2022). *Quirkos qualitative analysis software* [Computer software]. https://www.quirkos.com/

Regulation (EU) No 910/2014. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union, L 257*, 73–114. https://eur lex.europa.eu/eli/reg/2014/910/oj/eng

Regulation (EU) 2024/1183. (2024). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. *Official Journal of the European Union*, L 1183. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202401183

Schwalm, S., & Alamillo-Domingo, I. (2021). Self-sovereign identity & eidas: a contradiction? Challenges and chances of eidas 2.0. Wirtschaftsinformatik, 58, 247-270.

Schwalm, S., Albrecht, D., & Alamillo, I. (2022). eIDAS 2.0: Challenges, perspectives, and proposals to avoid contradictions between eIDAS 2.0 and SSI.

https://www.researchgate.net/publication/361816018_eIDAS_20_Challenges_perspectives_and_propsals_to_avoid_contradictions_between_eIDAS_20_and_SSI

Schwalm, S. (2023): The possible impact s of the eIDAS 2.0 digital identity approach in Germany and Europe. Open Identity Summit 2023. Bonn: Gesellschaft für Informatik e.V. PISSN: 1617-5468. ISBN: 978-3-88579 729-6. pp. 109-120. Regular Research Papers. Heilbronn, Germany. 15.-16. June 2023 10.18420/OID2023_09

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering, 63*(5), 603 613. https://doi.org/10.1007/s12599-021-00722-y

Seegebarth, C., Bastian, P., & Kraus, M. (2024). *Enabling attribute attestations*. https://doi.org/10.1007/s11623-024-1916-z

SGS. (2024). *Benefits of ISO/IEC 17065 Accreditation*. https://www.sgs.com/en-id/news/2024/12/pca-2024-q4-what-are-the-benefits-of-iso-iec-17065-accreditation

Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A., & Ranise, S. (2022). The eIDAS regulation: a survey of technological trends for European electronic identity schemes. *Applied Sciences*, *12*(24), 12679. https://www.mdpi.com/2076 3417/12/24/12679

Shehu, A., Pinto, A., & Correia, M. E. (2019). On the Interoperability of European National Identity Cards. In P. Novais, J. J. Jung, G. Villarrubia González, A. Fernández-Caballero, E. Navarro, P. González, D. Carneiro, A. Pinto, A. T. Campbell, & D. Durães (Eds.), *Ambient Intelligence – Software and* 72 *Applications, 9th International Symposium on Ambient Intelligence* (Vol. 806, pp. 338–348). Springer International Publishing. https://doi.org/10.1007/978-3-030- 01746-0_40

Soler, F. S. (2018). *Platform and method of certification of an electronic notice for electronic identification and trust services (EIDAS)*. https://patents.google.com/patent/US10938802B2/en

Trio. (2024). *ISO/IEC 15408 Certification Overview*. https://www.trio.so/blog/iso-15408-certification

Turner, H. W. (2003). Standards and Certification. Electrical Engineer's Reference Book.

Williamson, O.E. (1998). Transaction Cost Economics: How It Works; Where It is Headed. *De Economist* 146, 23–58 (19). https://doi.org/10.1023/A:1003263908567

Wimmer, M. A., Boneva, R., & di Giacomo, D. (2018). Interoperability governance: A definition and insights from case studies in Europe. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 1–11. https://doi.org/10.1145/3209281.3209306

Yin, R. K. (2018). Case study research and applications: Design and methods (Sixth edition). SAGE.

Appendix 1 – Interview questions

Thesis title: Shaping of the national certification framework for the European Digital Identity Wallet (EUDIW)

Interview questions

Part

Planned duration: Approx. 1 hour

Interviewer: Inessa Victoria Mülts, E-Governance Technologies and Services MSc student

Interviewee's organization:

Introduction

1. Please describe your current position and main responsibilities.

2. Could you share how you are involved with the EUDI Wallet initiative and your role in its development?

Part 1: Correlation Between Current eID Practices and EUDIW Requirements

1. How do current eIDAS implementation/assessment practices support or align with the goals of the EUDIW certification?

2. What are the primary differences introduced by the EUDIW certification requirements compared to existing eIDAS practices, and what challenges do these differences pose?

3. What are some of the adjustments that current eID schemes would need to make to align with EUDIW?

Part 2: Designing the EUDIW Certification Framework

4. Who are the key stakeholders, and how should they be engaged in the design process to ensure effective collaboration and input?

5. To what extent should users/citizens be involved in the design process of the EUDIW certification requirements, and should they be included at all?

6. Who should take responsibility for coordinating and overseeing the development of the certification process to ensure it is completed effectively and on schedule?

7. From your perspective, what are the essential requirements/elements necessary for EUDIW certification in the context of the new eIDAS 2.0?

8. How might ENISA's certification framework influence the development and implementation of national certification schemes, particularly in terms of challenges and alignment?

9. What do you consider the most critical factors when designing an EUDIW certification framework, considering all aspects (technical, legal, etc.)?

10. What are your recommendations for developing this certification scheme to ensure its effectiveness and sustainability?

Part 3: Challenges in Implementing the EUDIW Certification Scheme

11. In your opinion what do you see as the primary challenges in implementing the EUDIW certification scheme?

12. What measures are being proposed to address the main challenges in implementing the certification scheme, including areas such as data privacy, security, stakeholder collaboration, resource allocation, and regulatory compliance?

Additional Questions

13. Would you like to add anything regarding the development of the EUDIW certification framework that we haven’t discussed yet?

Appendix 2 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Inessa Victoria Mülts

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Shaping of The National Certification Framework for the European Digital Identity Wallet”, supervised by Dr. Silvia Lips
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

12.05.2025

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.