

DELFT UNIVERSITY OF TECHNOLOGY
MSc Management of Technology

MASTER THESIS PROJECT REPORT

Department of Engineering Systems and Services, Faculty of Technology, Policy and Management

April, 2026

Configuring Adoption in Regulated Digital Identity Ecosystems



Student: Magda Lamprinidou (4781309)

1st Supervisor: Prof.dr.ir. G.A. (Mark) de Reuver

2nd Supervisor: Dr.ir. Z. (Zenlin) Roosenboom-Kwee

Executive Summary

The roll-out of digital identity (ID) wallets presents a multi-sided adoption challenge embedded in a complex regulatory and ecosystem structure. While technical architectures have received significant attention, less is known about how wallet providers can strategically stimulate adoption among users and relying parties (RPs). This study addresses the question: *What adoption strategies could wallet providers consider when rolling out digital identity wallets?*

Digital ID wallets operate as two-sided platforms in which user adoption and RP integration are mutually dependent. Neither side generates value in isolation, creating a "chicken-and-egg" coordination problem that is further complicated by regulatory complexity, fragmented ecosystems, and uncertain demand. The European Digital Identity Wallet (EUDIW) represents the EU's regulatory effort to formalize wallet-based digital ID at scale, combining user control with interoperable, ecosystem-wide trust frameworks.

The study followed a three-stage research design. First, a targeted review of platform strategy, digital ID, e-government, and digital wallet literature was conducted, producing an initial set of strategy families organized into a layered adoption framework. Second, 18 semi-structured interviews were conducted with wallet and digital ID solution providers, ecosystem intermediaries (brokers), age verification (AV) experts, and representatives involved in EUDI initiatives, using the Gioia methodology to analyze the data. Third, AV was examined as a focused use case to test how the identified strategic domains apply under voluntary, regulation-triggered conditions.

The empirical analysis identified five interdependent strategic domains that wallet providers must configure in parallel to drive adoption: **institutional structuring of adoption** (addresses how providers navigate regulatory frameworks, certification requirements, and state involvement), **ecosystem orchestration & network activation** (addresses how providers activate RPs and partners to create user exposure; because users typically encounter the wallet through RP-embedded service flows, RP onboarding is the primary adoption lever and must precede consumer facing strategies), **user enablement & value proposition design** (addresses why users adopt and continue using the wallet; convenience and perceived usefulness consistently outweigh privacy and security concerns in routine adoption contexts), **incentive alignment & monetization architecture** (addresses how costs and incentives are distributed across market sides to stimulate growth; users expect wallet access to be free, making RP-side monetization and cross-subsidization models structurally necessary) and **trust & legitimacy construction** (addresses how credibility is established, particularly for RPs; trust functions asymmetrically: users prioritize convenience, while RPs require compliance assurance before integrating). In addition, the analysis identifies a sixth contextual dimension, **structural & market context conditions**, which captures exogenous factors such as cross-border regulatory fragmentation, cultural variation in institutional trust, and uneven market readiness that shape what adoption strategies are feasible. A central finding is that adoption does not emerge from isolated interventions but from the coherent configuration of all five domains simultaneously. Weaknesses in one domain constrain the effectiveness of the others, making adoption fundamentally a multi-sided coordination challenge rather than a single strategy problem.

Applying the framework to AV as a focused use case demonstrated that the configurational logic holds across different use case conditions, but each domain weightings shift substantially. In AV, institutional structuring becomes the dominant activation mechanism as regulatory enforcement substitutes for weak voluntary demand. Ecosystem orchestration is strongly RP-gated, user enablement shifts toward normalization and stigma management, and incentive alignment is constrained by limited willingness to pay and uncertain commercial viability. AV should therefore not be understood as an automatic precursor to broader wallet adoption, but as a regulation-triggered, platform-dependent entry point whose strategic value depends on enforcement intensity, governance credibility, and ecosystem integration.

For wallet providers, the framework serves as a diagnostic tool for identifying adoption bottlenecks and configuring mutually reinforcing mechanisms. Key priorities include establishing regulatory standing before market activation, prioritizing RP onboarding over consumer marketing, designing the wallet as free-to-user from the outset with monetization structured around RPs and high-assurance transactions, selecting use cases strategically for their frequency and habit-forming potential, and treating trust construction as an institutional priority rather than a UX feature. For consulting practitioners, the framework provides a shared conceptual reference for structuring strategic conversations with clients, aligning diverse stakeholders around a common understanding of adoption dynamics, and identifying where coordination failures are most likely to occur.

By re-conceptualizing digital ID wallet adoption as a configurational and institutionally embedded coordination process, this study extends existing theory in multiple ways. It shifts the analytical emphasis from layered causal sequences to configurational interdependence. It demonstrates that regulation can function as an active adoption trigger rather than a passive governance condition, substituting for missing early-stage network effects in voluntary markets. It reframes trust from a user-side behavioral variable to a multi-level coordination mechanism that operates differently for users and RPs. And it reframes incentive alignment from a tactical pricing decision to a structural cross-domain coordination mechanism that shapes participation dynamics across the entire ecosystem.

The resulting framework offers both theoretical refinement and practical guidance for wallet providers, intermediaries, and policymakers navigating the complex roll-out of digital ID infrastructures in Europe and beyond.

Contents

Nomenclature	iv
1 Introduction	1
1.1 Context	1
1.2 Problem Statement	2
1.3 Research Objective	2
1.4 Research Question	2
1.5 Research Scope	2
1.6 Theoretical Background	3
1.6.1 Digital Identity as a Platform Context	3
1.6.2 Platform Theory	5
1.6.3 Research Gap	6
1.7 Research Methodology	6
1.8 Thesis Structure	7
2 Literature Review and Strategy Synthesis	8
2.1 Stage 1: Methodology	8
2.2 Literature Findings	9
2.2.1 Adoption Strategies from Multi-sided Platform Literature	9
2.2.2 Adoption Strategies from Digital Identity and eID Literature	11
2.2.3 Adoption Strategies from Digital Wallet and Payment Literature	13
2.3 Synthesized Strategy Families & Conceptual Framework	13
2.3.1 From Individual Mechanisms to Strategy Families	13
2.3.2 From Strategy Families to a Layered Adoption Framework	15
3 Empirical Research Methodology	16
3.1 Stage 2: Expert Interviews	16
3.1.1 Research Ethics	17
3.1.2 Sampling Strategy	18
3.1.3 Data Collection	19
3.1.4 Data Pre-Processing	19
3.1.5 Data Analysis	20
3.2 Stage 3: AV Use Case	22
4 Results: A Multi-Domain Framework of Wallet Adoption Strategies	23
4.1 Strategy Dimensions	23
4.1.1 Institutional Structuring of Wallet Adoption	23
4.1.2 Ecosystem Orchestration & Network Activation	25
4.1.3 User Enablement & Value Proposition Design	28
4.1.4 Incentive Alignment & Monetization Architecture	30
4.1.5 Trust & Legitimacy Construction	32
4.2 Contextual Dimension	34
4.3 Framework	36
4.4 Discussion	38
5 Age Verification (AV) as a Use Case	40
5.1 Introduction: AV as a Regulation-Triggered Use Case	40
5.2 Regulatory Context: Enforcement as Market Trigger	40
5.3 Conceptual Distinction: Age Assurance (AA) vs. Identity Assurance (IDA)	40
5.3.1 Technical Approaches to AA	41
5.4 Strategic Positioning: Standalone Application or Wallet-Integrated Feature?	41
5.5 Analytical Synthesis	42
5.6 Applying the Multi-Domain Framework to AV	42
5.7 Summary	44

6	Extended Discussion	45
6.1	The Debate in Digital Identity Ecosystems: Should the user be free?	45
6.2	Identity and Payments: Two Distinct Strategic Debates	45
6.2.1	Payments as a Use Case within Digital Identity Wallets	45
6.2.2	Should Identity Ecosystems Be Approached Like Payment Ecosystems?	45
6.3	Applicability of the Framework to Government-Issued Wallets (EUDIW)	46
6.4	Boundary Conditions of the Multi-Domain Framework	47
7	Implications and Conclusions	48
7.1	Managerial Implications	48
7.2	Limitations and Reflexive Considerations	48
7.3	Future Outlook	49
7.4	Conclusions	50
	Acknowledgments	52
	Use of AI Tools	52
	References	53
8	Appendix	56
8.1	Adoption Strategies from Literature	56
8.2	Interviewee List	57
8.3	Interview Guides	58
8.3.1	Interview Guide – Digital Identity Experts	58
8.3.2	Interview Guide – Age Verification Experts	61
8.4	Informed Consent Form (ICF)	63

List of Figures

1	Platform Network Model	4
2	The Wallet-Based Model	5
3	Conceptual framework	16
4	Strategy Dimension 1	24
5	Strategy Dimension 2	26
6	Strategy Dimension 3	28
7	Strategy Dimension 4	31
8	Strategy Dimension 5	33
9	Contextual Dimension	35
10	Configurational Framework of Wallet Adoption	37

List of Tables

1	Literature-derived strategy families and representative mechanisms.	14
2	Mapping of the layered framework to the interview guide	17
3	List of Adoption Strategies from Literature	56
4	Interview Participant Anonymization List.	57

Nomenclature

Abbreviations

2FA	Two-Factor Authentication
AA	Age Assurance
AE	Age Estimation
AI	Age Inference
AV	Age Verification
DIB	Digital Identity Broker
DIP	Digital Identity Provider
DISPs	Digital Identity Service Providers
DMP	Data Management Plan
DSA	Digital Services Act
eID	electronic Identity
eIDAS	Electronic Identification, Authentication, and Trust Services
EU	European Union
EUDI	European Digital Identity
EUDIW	European Digital Identity Wallet
HREC	Human Research Ethics Committee
ICF	Informed Consent Form
ID	Identity
IDA	Identity Assurance
IdM	Identity Management
mDL	mobile Driver's License
MVP	Minimum Viable Product
NDID	National Digital Identity
RP	Relying Party
SUA	Strong User Authentication
UK	United Kingdom
US	United States
UX	User Experience
WP	Wallet Provider

1 Introduction

1.1 Context

In the digital era we live in, with communications and social interactions often occurring through screens and algorithms, the notion of identity (ID) has shifted significantly: originally rooted in the Latin *idem* (“the same”) (Online Etymology Dictionary, [n.d.](#)), identity is a many-sided concept with personal, political, and legal definitions (Krotoski & Hammersley, 2015) and is understood differently across disciplines. Identity balances notions of sameness and difference, which seems simple in theory but is complex in practice (Coulmas, 2019). As identity moves from a broad social and legal concept into digital environments, the term *digital identity* has emerged. Therefore, it becomes essential to examine how people themselves understand and use the idea of “*digital identity*” in everyday life. Rowland and Stevens (2025) showed in their qualitative work that users interpret digital identity in three ways: as *digital identification*, as *self-presentation*, and as the “*datafied*” *self*. These views are fluid and often overlap, indicating that identification mechanisms, online user personas, and user’s data gathered by platforms together form one’s digital identity. From an information systems perspective, digital identity is often mentioned when referring to *identification* (personal identity affirmation), *authentication* (identity verification), and *authorization* (determining resource access rights) (Dutch Payments Association, 2025; Rowland & Stevens, 2025); this view complements the user perspectives by focusing on the technical mechanisms that make digital identities operational.

Identity-management (IdM) systems are used for the challenging work of providing secure and reliable authentication for users (Podgorelec et al., 2022). Multiple IdM models exist, however, and as digital identity becomes more layered and data-driven, concerns about privacy, security, and who controls the data have grown. This has created a shift toward user-centric models, which aim to place users in control of their digital identity data (Podgorelec et al., 2022). The *digital identity wallet* is one such user-centric model. Podgorelec et al. (2022) describe digital identity wallets as software that “*enables the storing, managing, and sharing of digital identity-related data*” and that also provides “*secure storage for cryptographic material associated with digital identity-related data*” (pg. 816). They argue that the “*primary motivations for applying digital wallets to the digital identity domain are to avoid digital identity related data centralization, enhance the security and privacy of identity-related data, provide control over identity-related data under user responsibility, and ease the use of digital identities*” (Podgorelec et al. (2022), pg. 815). Furthermore, according to Podgorelec et al., a wallet should allow users to review and remove identity stored data, selectively combine and disclose identity elements when sharing, and support backup and recovery in the underlying environment. In short, digital identity wallets operationalize the user-centric shift by offering individuals a single, controllable tool to manage the layered, datafied identities described by Rowland and Stevens, while directly addressing the privacy, security, and governance concerns that started the move away from other non-user centric IdM models.

Because of this, policymakers have begun to formalize this model at scale. In the European Union (EU), the eIDAS 2.0 legislation (European Union, 2024a) introduces the European Digital Identity Wallet (EUDIW) (European Commission, 2025c), which member states must make available to “*legal persons*” (citizens, residents, and organizations) on a voluntary basis while placing a reciprocal obligation on many public and private relying parties (RP) to accept the wallet for processes that require strong user authentication (SUA) (or two-factor authentication, 2FA) (Dutch Payments Association, 2025), thereby aligning user choice with regulatory support for interoperable, wallet-based identity flows.

One practical application of the EU wallet concept is age verification (AV). The European Commission has specified a mobile “age verification” app that functions as a digital wallet to hold a user’s proof of age and enable access to age-restricted online content (European Commission, 2025a; Windwehr & Hancock, 2025). After installation of the app, users can obtain age attestation through multiple channels, such as national ID schemes, physical ID cards, linkages to other apps that already hold age data (for example, banking apps), or third-party assessments provided by entities such as banks or notaries. The app will then generate a verifiable proof of age that users can present to websites: when a platform requests age confirmation, the wallet supplies the attestation so the user can access restricted content (Windwehr & Hancock, 2025). Importantly, the EU intends for this AV solution to be compatible with and integrable into the broader EUDIW architecture and considers this app as a practical precursor (called the “*mini wallet*”) of the EUDIW (European Commission, [n.d.](#)). Therefore, AV is a focused, concrete use case that demonstrates how digital identity wallets can carry verifiable attestations and interact with online platforms.

However, unlike many regulated contexts where SUA is required and RPs will be obliged to accept EUDI wallet-based credentials, AV typically does not demand SUA. This difference matters because adoption dynamics change when users can opt in freely and platforms on the other side of the market are not compelled to accept a new method. In other words, wallets operate in a two-sided environment: end-users who must be willing to install and use a wallet, and RPs/platforms who must accept and integrate it (Aziz, 2025). The incentives and frictions for each side differ depending on whether adoption is mandatory or voluntary.

Since the EUDIW is not yet broadly deployed (many pilots are underway (European Commission, 2025d)), the roll-out can only rely on lessons from prior and existing digital ID initiatives. Studying adoption strategies from those initiatives and testing how they translate to a voluntary, platform-driven use case such as AV is therefore essential to inform policy

and design choices for the EUDIW.

1.2 Problem Statement

There is limited empirical evidence on how wallet providers and ecosystem actors approach user adoption when introducing digital ID wallets, especially in voluntary use cases where platforms are not legally compelled to accept wallet-based credentials. Age verification (AV), as a precursor to the EUDI Wallet, is an example of this voluntary, two-sided challenge: the user side must adopt and trust the wallet, while the platform side must choose to accept and integrate it. Given the current stage (pilots and fragmented past initiatives), understanding the adoption strategies considered by wallet providers is necessary to design roll-outs that achieve uptake across both sides of the market and ensure the practical viability of the EUDIW.

For wallet providers, adoption is not only a policy or compliance goal but determines ecosystem viability. Wallet providers and intermediaries depend on adoption to sustain their operations through compensation per verification request, contractual revenues from relying parties (RPs), or public funding linked to usage metrics (Aziz, 2025). Without sufficient reach, the providers' economic and operational models collapse, and the broader wallet ecosystem cannot reach large-scale adoption. In addition, successful adoption in one use case, such as AV, could potentially produce spillover effects into adjacent use cases (e.g. electronic signing, accessing government services and payments (European Commission, 2025b)) increases the wallet's overall value proposition and market relevance.

From a research perspective, digital ID wallet adoption differs fundamentally from adoption of conventional digital systems. First, it takes place within a two-sided platform structure, where value depends on the simultaneous participation of both users and RPs. This interdependence creates the well-known “*chicken-and-egg*” problem: users will only adopt if enough RPs accept wallets, while RPs will only integrate if enough users are active (Caillaud & Jullien, 2003; Liezenberg et al., 2019). In addition, wallets operate in a regulated trust environment, where participation depends on compliance and certification, adding regulatory dynamics absent from most consumer technologies. Lastly, voluntary use cases such as AV differ from mandated ones (SUA in banking): neither side is legally obliged to participate, making strategic planning, trust, and perceived value critical to drive adoption.

These characteristics make wallet adoption a distinct socio-technical problem that bridges technology acceptance, platform ecosystem coordination, and governance design. Investigating how wallet providers approach adoption in voluntary, two-sided settings is therefore both scientifically relevant and practically essential to ensure the long-term success and sustainability of the EUDIW.

1.3 Research Objective

This research aims to develop a structured understanding of adoption strategies for digital ID wallets in two-sided, regulated ecosystems. The study aims to produce a multi-domain framework that identifies, categorizes, and explains the strategic mechanisms through which wallet providers stimulate participation among users and RPs. Age verification (AV) is examined as a focused use case to demonstrate how the framework can be applied diagnostically to derive context-specific strategic priorities in a setting where voluntary demand is weak and regulatory enforcement is the primary activation mechanism of adoption.

1.4 Research Question

The central research question in this study is:

What adoption strategies could wallet providers consider when rolling out digital identity wallets?

To address this main question, the following sub-questions will be explored:

- RQ1: What adoption strategies emerge from the literature and past digital identity and wallet initiatives?
- RQ2: How do expert practitioners evaluate, validate, and enrich this framework?
- RQ3: How applicable are the validated adoption strategies to a voluntary, platform-dependent use case, specifically age verification (AV) as a precursor to the EUDIW, and what AV-specific measures should wallet providers consider?

1.5 Research Scope

This study focuses on adoption strategies for digital ID wallets from the perspective of wallet providers and ecosystem orchestrators operating within the EU regulatory context, with particular reference to the EUDIW under eIDAS 2.0. The primary geographic focus is the EU, with targeted inclusion of UK-based perspectives where they offer relevant comparative insights into regulatory enforcement and AV market development. The study focuses on strategic and

organizational dimensions of adoption. Technical and architectural details of wallet infrastructure, such as cryptographic protocols, credential formats, or system interoperability standards, are outside the scope of this research. Similarly, the study does not aim to measure consumer behavior or quantify adoption rates, but rather to understand the strategic choices and mechanisms through which ecosystem actors pursue adoption. The analysis draws on expert perspectives from wallet providers, identity brokers/intermediaries, and ecosystem orchestrators. While policymaker perspectives are included where relevant, the primary unit of analysis is the wallet provider operating within a regulated ecosystem. AV is examined as a focused use case within this scope, selected because its characteristics (weak voluntary demand, strong regulatory dependency, and RP-mediated adoption) allow the developed framework to be examined under particularly demanding conditions. The study does not aim to evaluate specific national implementations or compare country-level roll-out trajectories in depth. Where international examples are referenced (such as Singapore’s Singpass) these are used illustratively to inform strategic insights rather than as objects of comparative analysis. Within the digital wallet literature, the study draws on insights from payment wallet adoption research where relevant, as both payment and ID wallets operate as platform infrastructures subject to indirect network effects and cross-side coordination challenges. Cryptocurrency wallets are outside the scope of this study, as their adoption dynamics, governance structures, and user contexts differ fundamentally from the regulated, government-backed ID infrastructure examined here.

Furthermore, several actor groups and domains are explicitly outside the scope of this study. First, RPs (the organisations and platforms that consume verified ID attributes) were not interviewed as experts. Their perspectives are represented indirectly through the accounts of wallet providers and intermediaries, but RP adoption dynamics are not examined as a standalone focus. Second, end users of digital ID wallets are outside the scope of this study. The research does not examine individual user behavior, acceptance, or experience directly, but rather how wallet providers strategically address user-side adoption challenges. Third, the study focuses on independent wallet providers and ecosystem orchestrators. Third, the study focuses exclusively on wallets designed for natural persons. Business ID wallets, which serve organizational rather than individual ID needs, are outside the scope. Finally, the emerging topic of digital ID for AI agents is outside the scope of this study, as this represents a newly emerging and distinct domain that goes beyond the current EUDIW framework and the adoption challenges examined here.

1.6 Theoretical Background

The following section introduces the theoretical foundations that inform the analytical approach of this study. It first situates digital ID wallets within a platform context, then presents two-sided market and network effect theory as the conceptual lens through which adoption challenges are examined, and concludes by identifying the research gap this study addresses.

1.6.1 Digital Identity as a Platform Context

Digital ID has evolved from isolated login mechanisms (multiple user names and passwords) into interconnected identity ecosystems that ensure trust between **users**, **issuers**, and **service providers** (McLaughlin et al., 2009). In these ecosystems, the digital ID of an actor consists of collections of contextual data and verifiable claims. Platforms that manage such data effectively transform digital ID itself into a platform proposition (**identity platforms**): they enable digital interactions by verifying and exchanging trust between distinct parties (Liezenberg et al., 2019). As digital interactions have multiplied over the last years, a market for digital trust intermediaries has emerged. Many actors such as national electronic identity (eID) schemes (e.g. DigiD (DigiD, 2025)), initiatives from banks (e.g. iDIN (iDIN, 2025)) and private Big Tech providers (e.g. Google (Google, 2025), Apple (Apple Inc., 2025)) offer digital ID services. This results in a fragmented identity landscape, in which users have multiple credentials (user names and passwords) and service providers (relying parties, RPs) need to connect to and manage multiple different digital ID systems, each with its own technical and operational requirements. (Liezenberg et al., 2019).

Identity Platform Models

In order to address the fragmentation and scale trust, ID intermediaries operate as digital platforms that connect two user groups: end-users and RPs. According to Liezenberg et al. (2019), four recurring identity platform models can be distinguished:

- **Direct model:** RPs issue their own credentials directly to users. This increases governance but maintains fragmentation.
- **Hub model:** Large actors (such as governments, social media or bank platforms) open their authentication systems for external use, offering reach but centralizing governance.
- **Network model:** Multiple digital ID providers (DIPs), or else, issuers cooperate in federated networks. This reduces fragmentation through mutual recognition of users and shared standards.

- **Aggregator (gateway) model:** Digital Identity Service Providers (DISPs) (such as Signicat (Signicat, 2025)) aggregate several identity platforms on one interface, lowering integration costs for RPs and improving reach.

Therefore, each model balances governance, interoperability, and market reach differently, but all create value by enabling trusted exchanges rather than by owning user data or credentials.

Among the four models, the **network model** is most relevant to this study because it captures the principle of federated interoperability across multiple DIPs. This model is illustrated in figure 1, which shows how users and RPs (highlighted in red) each connect to their respective digital ID providers (DIPs), while the providers interoperate within a shared trust network (DIPs recognize each other's credentials) as indicated by the blue dashed boundary. The red highlighting draws attention to the two sides of the market (users and RPs) whose simultaneous participation is necessary for the network to function. Each DIP serves both market sides, while network interoperability allows users to authenticate across RPs to verify IDs issued elsewhere (Liezenberg et al., 2019).

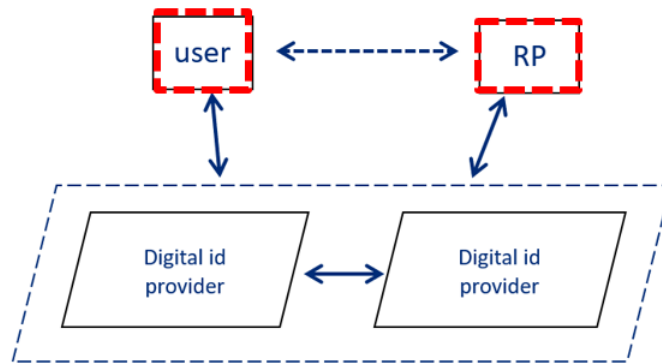


Figure 1: The Platform Network model of digital ID. Users and RPs interact via multiple digital ID providers (DIPs) that interoperate within a shared trust network. Each DIP acts as a node in the network, enabling credential exchange while maintaining its own user and RP relationships. (Adapted from *Everything Transaction* (1st English ed., pg. 213), by Liezenberg et al. (2019), INNOPAY International.)

From Platform Networks to Regulated Wallet Ecosystems

Building on this foundation, the EUDIW introduced under eIDAS 2.0 regulation is an evolution of the platform network model into a **regulated network platform**. Rather than a single centralized service, the EUDI Wallet is a federated ecosystem of interoperable wallets and issuers (DIPs) operating under common trust and governance standards. The wallet-based model (figure 2) expands the market-oriented network of figure 1 (the same two sides of the market, users and RPs, are again highlighted in red, preserving the two-sided dynamic) by adding institutional trust mechanisms (the regulator and trust registry) which certify and monitor ecosystem participants (Kudra et al., 2025). Users request attestations from issuers, store them in their wallet, and present them to RPs (service providers in figure) to access services. The trust registry keeps a list of certified issuers and RPs (trust lists), ensuring that only authorized entities can participate in the network (Kudra et al., 2025). Therefore, this regulated wallet ecosystem, institutionalizes interoperability while preserving the core two-sided dynamic between users and RPs.

This regulated structure is analytically important because it introduces institutional constraints (certification requirements, trust frameworks, and governance obligations) that shape what adoption strategies are feasible. Standard platform adoption mechanisms (such as seeding or asymmetric pricing) must therefore be reconsidered within this governed environment. This tension between platform logic and regulatory structure forms the central analytical problem of this study.

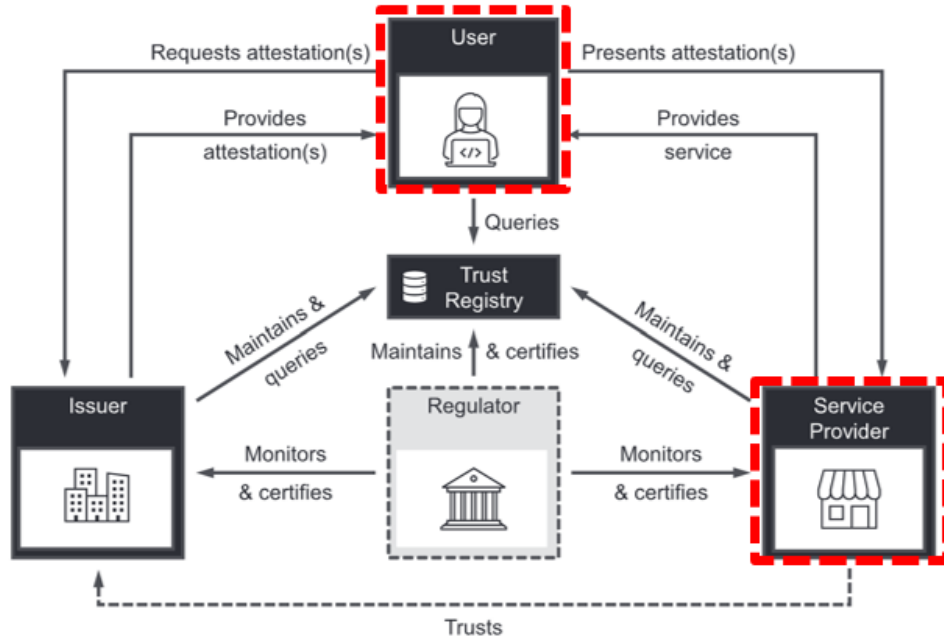


Figure 2: The wallet-based model. The EUDIW architecture extends the Platform Network model by embedding governance and certification layers (regulator and trust registry) that maintain trust across users, issuers, and RPs. (Adapted from *Digital Identity Wallets: A Guide to the EU’s New Identity Model* (pg. 3), by Kudra et al. (2025), Information Systems Journal, John Wiley & Sons Ltd. CC BY license.)

1.6.2 Platform Theory

The previous section described how digital ID ecosystems operate according to platform logic, connecting users and RPs through interoperable intermediaries. Platform theory provides the conceptual foundation for understanding these dynamics. In general, a platform is an intermediary that enables interactions (or transactions) between two or more different interdependent user groups. Rather than producing goods or services directly, identity platforms create value by enabling connections, exchanges, and co-creation among participants (Liezenberg et al., 2019).

Two-Sided Market Dynamics

In two-sided markets, the demand of one user group depends on the participation of another. A platform must therefore attract both sides simultaneously (users and RPs) because neither side creates value in isolation (Rysman, 2009). This interdependence gives rise to the so-called “**chicken-and-egg**” problem of platform adoption: users will only adopt if enough RPs participate, while RPs will only integrate if enough users are active (Caillaud & Jullien, 2003; Schlatt et al., 2022). In order to overcome this, platform operators implement asymmetrical value propositions distinct incentives, pricing structures, or benefits specific and different for each side of the market (Rysman, 2009). In the case of digital ID, this means that wallet providers must appeal to users through trust, privacy protection, and convenience, while convincing RPs through low integration costs, interoperability, and compliance benefits (Liezenberg et al., 2019).

Network Effects and Platform Growth

Network effects is the phenomenon which occurs when the value of a service increases with the number of its users (Katz & Shapiro, 1985) and is central to platform theory. Two types can be distinguished: **cross-side network effects** (which occur when additional participants on one side increase the platform’s utility for the opposite side) and **same-side network effects** (which arise within one user group), both either positively (e.g. reputation sharing among trusted RPs) or negatively (e.g. competition among RPs). The strength and direction of these effects determine whether a platform reaches the “tipping point” where adoption becomes self-sustaining. In two-sided identity markets, such as those described by Liezenberg et al. (2019), achieving this critical point depends on strategy: securing partnerships, offering incentives or subsidies to one side, and lowering onboarding friction.

Although classic platform theory assumes market-driven coordination, the EUDIW operates within a regulated, federated network. As discussed in section 1.6.1, governance functions are distributed across the trust registry and regulator.

Regulation in this context has two key roles: it reduces uncertainty by certifying trustworthy participants (lowering the perceived risk for early adopters) and it creates coordination (potentially promoting adoption through public-sector participation or mandates in specific use cases (e.g. AV)). However, regulation does not eliminate the underlying two-sided interdependence between users and RPs. The wallet’s success still depends on voluntary participation and cross-side network effects. Therefore, the chicken-and-egg problem persists, but within a governed environment (Aziz, 2025).

In summary, the EUDIW is a case of a regulated two-sided platform, where adoption is driven by network effects, mediated by trust, and sustained by governance. Traditional adoption models, which focus on individual user acceptance factors, are insufficient to capture this complexity. Instead, platform and network theories provide the analytical lens to understand how wallet providers can avoid coordination failures, and enable sustainable, large-scale adoption of digital ID ecosystems in Europe.

1.6.3 Research Gap

Despite growing policy and pilot projects around the EUDIW, academic research on wallet adoption remains scarce. Most of the available knowledge is from theses, practitioner blogs, and EU pilot documentation, such as those linked to the *IMPULSE* project (Jackwerth-Rice et al., 2023) and early AV trials (e.g. Age Check Certification Scheme (2025)). These sources offer practical insights but lack a consolidated theoretical understanding of how wallet providers can achieve adoption across both sides of the market.

Among the Master’s thesis studies, Aziz (2025) examines the creation and governance of digital ID wallet ecosystems, showing that wallet providers face a chicken-and-egg problem between users and relying parties (RPs). He identifies different strategic orientations (publicly governed, corporate, and niche wallet providers) but focuses mainly on business models and ecosystem formation, not on adoption strategy itself. Kudra et al. (2025) similarly highlight organizational and technical barriers that slow adoption, emphasizing ecosystem immaturity and interdependence between issuers, verifiers, and users. Their work confirms that adoption challenges persist even with regulatory backing.

At the national level, the Master’s thesis of Tanriverdi (2025) provides one of the first empirical analyses of EUDIW implementation in Estonia and Belgium, showing that differing governance models, certification delays, and citizen awareness hinder adoption. However, his study focuses on institutional rollout rather than the strategic actions of wallet providers. Complementary user studies, such as Murtezaj (2023), underline that trust, usability, and operator reputation strongly shape individual acceptance, yet these micro-level factors are rarely linked to broader market coordination.

In general, the literature indicates that EUDIW adoption is influenced by technical, organizational, and governance conditions, but empirical evidence on adoption strategies by wallet providers, especially in voluntary, two-sided contexts (such as AV) is limited. This study addresses this gap by examining how wallet providers approach adoption as a strategic problem, developing a framework grounded in prior initiatives, and expert perspectives.

1.7 Research Methodology

For this research, a qualitative, exploratory methodology was applied in order to investigate strategies for driving the adoption of digital identity wallets, with a particular focus on online age verification as an early and voluntary use case. The research is characterized by regulatory complexity, multi-actor ecosystems, and strong inter-dependencies between different sides of the market. Given the novelty of the EUDIW ecosystem and the limited empirical literature on adoption strategies in such regulated, multi-provider environments, an exploratory qualitative approach is considered appropriate.

Digital identity wallets operate within a two-sided market structure, where adoption by end users is closely linked to adoption by RPs, and vice versa. Understanding how adoption strategies are conceived, prioritised, and implemented therefore requires access to expert knowledge and experience rather than measurements. Qualitative research allows for an in-depth examination of strategic decision-making processes, trade-offs, failures, and contextual constraints that are difficult to capture through quantitative methods. This approach is well aligned with prior research in digital platforms, information systems, and digital identity, which frequently relies on expert interviews to explore emerging socio-technical systems (Degen & Teubner, 2024; de Reuver et al., 2018).

Research Design

The research design of this study followed a structured, three-stage qualitative process that aligns directly with the research objectives. The aim of the design was to develop a grounded understanding of adoption strategies for digital identity wallets by combining insights from existing literature with empirical evidence from practitioners, and by testing these strategies within the specific, voluntary use case of age verification.

The research design stages are:

- Stage 1: Targeted review of literature and past digital ID initiatives to generate an initial set of potential adoption strategies.

- Stage 2: Semi-structured interviews with experts to validate, challenge and enrich those strategies.
- Stage 3: Focused inquiry into the AV use case to test which strategies apply in a voluntary, platform-dependent setting and to surface AV-specific recommendations for wallet providers and policymakers.

The first stage of the research focused on a targeted review of academic literature, policy reports, and documented digital identity initiatives. This stage was necessary to establish a theoretical baseline and to identify existing adoption mechanisms and strategic patterns discussed across the domains of digital identity, two-sided platforms and digital wallet/payment systems. Given the fragmented nature of the literature across these fields, insights from this review were synthesized into a set of literature-derived strategy families, which formed the conceptual foundation of the study.

The second stage consisted of semi-structured expert interviews with practitioners involved in digital identity wallets, trust services, age verification solutions, and related ecosystem roles. This stage was included to complement and critically assess the literature-derived strategies through practitioner perspectives. Expert interviews are particularly suited for capturing contextual detail, trade-offs, and implementation challenges that are often underrepresented in formal reports. By talking to practitioners responsible for strategic decision-making, this stage enabled the study to validate, challenge, and refine the strategies identified in the literature.

The third stage focused specifically on digital age verification as a voluntary and platform-dependent use case within digital identity wallets. This stage was designed to test the applicability of the identified adoption strategies in a context characterized by increased sensitivity to privacy, regulatory complexity, and strong interdependencies of the two sides. Age verification was selected because it represents a critical yet non-mandatory use case (in the EU), making it especially suitable for examining adoption dynamics in the absence of legislation mandating the uptake mechanisms.

Together, the three stages form an integrated research design that combines theoretical synthesis with empirical inquiry. Triangulating literature evidence with practitioner experience produces a grounded, actionable framework designed to inform wallet roll-out practice and EUDIW policy choices. The qualitative approach prioritizes depth and contextual understanding so the final framework captures not only which adoption options exist, but why actors choose them and how those choices play out in practice.

1.8 Thesis Structure

The remainder of this thesis is structured as follows:

Chapter 2 presents the findings of Stage 1 of the research, covering adoption strategies from three domains (multi-sided platforms, digital identity and eID systems, and digital wallet and payment systems) and synthesizing these into a layered adoption framework. Then, chapter 3 describes the empirical research methodology of Stage 2 and Stage 3, including the expert interview design and the approach taken for the AV use case. Chapter 4 presents the empirical results of Stage 2 in the form of a multi-domain framework of wallet adoption strategies, consisting of five strategic dimensions and one contextual dimension, followed by a discussion of the theoretical contributions. Chapter 5 presents the results of Stage 3, examining AV as a focused use case and applying the multi-domain framework to assess how strategic priorities shift under conditions of weak voluntary demand and strong regulatory dependency. Chapter 6 presents an extended discussion of broader debates surfaced by the findings, including the tension between free-to-user wallet models and commercial sustainability, the relationship between ID and payment ecosystems, and the boundary conditions of the framework. Finally, chapter 7 presents the managerial implications, limitations, future outlook, and overall conclusions of the study. Supporting materials are provided in the appendix 8.

2 Literature Review and Strategy Synthesis

This chapter presents the literature research part of the study. It first explains how the targeted literature review and synthesis were conducted in Stage 1 of the research (chapter 2.1). It then presents the key findings from three relevant literature strands: multi-sided platforms, digital identity and eID research, and digital wallet and payment literature (chapter 2.2). Finally, the chapter synthesizes these insights into higher-level strategy families and an initial conceptual framework of digital ID wallet adoption (chapter 2.3). In this way, the chapter moves from literature review method, to literature findings, to conceptual synthesis.

2.1 Stage 1: Methodology

The literature review was conducted through a targeted and iterative search strategy aimed at identifying adoption strategies relevant to digital identity wallets as regulated, multi-sided platforms. The review was designed to integrate insights from platform strategy, digital identity and e-government research, and digital wallet adoption studies, rather than to provide an exhaustive systematic review.

As an initial foundation, the review included a small number of seminal books and practitioner-oriented works on platform strategy and multi-sided markets, including strategy-focused texts such as D. S. Evans and Schmalensee (2016) and Parker et al. (2016) and related literature on platform economics and coordination problems (e.g. industry book by Liezenberg et al. (2019)). These sources were used to establish core concepts such as indirect network effects, chicken-and-egg dynamics, asymmetric pricing, and platform launch strategies, which informed the analytical lens applied throughout the study.

Academic literature searches were primarily conducted using *Google Scholar*, complemented by targeted searches in publisher databases where appropriate. The search process began with broad queries related to platform economics and two-sided markets, using combinations of terms such as *two-sided platform*, *multi-sided platform*, *user adoption*, *user onboarding*, *critical mass*, and *chicken-and-egg problem*. The term *wallet* was also included where relevant to capture platform discussions specifically addressing digital wallet contexts. This stream of literature was used to identify general strategic mechanisms for overcoming early adoption barriers.

Building on this foundation, the search strategy was refined to focus on platform launch and growth strategies. Keywords such as *platform seeding*, *bootstrapping*, *subsidising one side*, *cross-side pricing*, *marquee users*, *referral programs*, and *achieving critical mass* were used to identify studies examining concrete adoption tactics in multi-sided settings. This stream included peer-reviewed journal articles, conference papers, and selected master's theses where these provided detailed empirical or conceptual insights into platform adoption dynamics.

A third stream of literature focused specifically on digital identity systems, federated identity infrastructures, and e-government initiatives. Searches combined terms such as *digital identity*, *federated identity*, *self-sovereign identity*, *identity federation*, *verifiable credentials*, and *decentralised identifiers* with *user adoption*, *user onboarding*, *usability*, *trust*, and *privacy*. Particular attention was given to government-led and regulator-driven schemes, including national digital identity programs and e-government initiatives, using keywords related to *trust frameworks*, *regulation*, *eIDAS*, and public-sector identity infrastructures. Case-based studies of large-scale deployments, such as *Aadhaar*, *GOV.UK Verify*, and *European eID* initiatives, were included to capture lessons regarding adoption barriers, institutional trust, and privacy perceptions. In addition, a complementary stream of literature examined digital wallet and payment system adoption. Searches included terms such as *digital wallet adoption*, *e-wallet diffusion*, *user adoption*, *merchant adoption*, and *interoperability*. Although payment wallets differ functionally from identity wallets, both operate as intermediary infrastructures connecting multiple sides of a market and are subject to indirect network effects and coordination challenges (Liezenberg et al., 2019). This stream was therefore used to complement platform and eID research with empirical insights into incentive structures, merchant/RP onboarding, and cross-side participation dynamics. It is noted that the focus was primarily on payment and e-wallet literature. Cryptocurrency wallets (blockchain-based wallets) were outside the scope of this review, as they operate under fundamentally different adoption logics, governance models, and user incentives. However, one hybrid wallet model that combines digital ID and wallet functionalities (Worldcoin) was included since it provides relevant insights into ID-related adoption dynamics (Kraiwanit et al., 2023).

Throughout the review process, literature selection and analysis were iterative rather than linear. Abstracts were first screened for relevance, after which selected papers were read in more depth and documented in a structured review file. For each paper (or relevant book chapter), key information was recorded, including: (1) the adoption problem addressed, (2) the strategic mechanism proposed or observed, (3) the target actor group (users, RPs, or system-level actors), (4) adoption determinants discussed (if any), and (5) contextual factors influencing effectiveness.

Rather than applying formal qualitative coding software, the analysis followed a manual thematic comparison approach. Identified strategies were initially extracted as discrete mechanisms (e.g., *piggybacking*, *seeding*, *micro-market focus*, etc.). In parallel, recurring behavioral (and organizational) determinants of adoption (e.g. *perceived trust*, *perceived usefulness*, *ease of use*, etc.), were consolidated across studies. While much of the digital identity literature focuses primarily on

such determinants rather than explicit strategies, these factors were retained in the analysis because they represent the micro-level mechanisms through which strategic interventions influence adoption decisions.

The extracted strategies were then compared across the literature strands to identify recurring functional patterns. In particular, attention was paid to the type of adoption challenge addressed (e.g., coordination failure, trust deficit, integration cost, regulatory uncertainty) and to the level at which the mechanism operates (user-side, RP-side, or ecosystem level). Through iterative comparison, conceptually similar mechanisms were grouped into higher-level categories. For example, strategies such as *seeding*, *piggybacking*, and *micro-market focus* were clustered as "early-stage network activation strategies", while *asymmetric pricing*, *penetration pricing*, and *freemium* models were grouped under "pricing and incentive strategies". Also, the relationship between strategy categories and adoption determinants was examined in order to develop a layered conceptual structure. This process resulted in literature-derived strategy families organised within a framework that distinguishes between governance conditions, strategic interventions, adoption determinants at the micro-level, and cross-side network effects. In this way, the synthesis moved from individual strategies and determinant findings identified in specific studies to a structured understanding of how different mechanisms interact within multi-sided digital identity ecosystems.

The full list of extracted strategies and their description is provided in the appendix 8.1 for transparency. The main text below presents the synthesized strategy families and determinants that emerged from this comparative analysis (see chapters 2.2-2.3).

2.2 Literature Findings

In this thesis, adoption strategies are defined as deliberate strategic choices and interventions taken by wallet providers to influence participation and usage within the digital ID ecosystem. These strategies address challenges such as coordination failures, trust concerns, integration costs, and unclear value propositions. Adoption strategies should be distinguished from adoption determinants, which describe factors influencing participation decisions (e.g., perceived usefulness, trust, or cost). Strategies represent the mechanisms through which providers shape, address, or leverage these determinants, when designing and deploying wallet solutions.

Digital identity wallets can be understood as multi-sided platforms that coordinate interactions between at least three groups of actors: end-users, credential issuers, and RPs. In this research context, RPs include both online platforms and other service providers that wish to consume verified identity attributes, while the wallet provider mediates these interactions within a regulated ecosystem. As the platform literature emphasizes, such multisided arrangements are particularly exposed to demand-side adoption challenges: neither side is willing to join unless the other side is sufficiently present, leading to "chicken-and-egg" coordination problems and critical mass thresholds that can be hard to cross (D. Evans & Schmalensee, 2010). At the same time, research on e-government, national digital ID (NDID) systems, and digital wallets shows that adoption is also constrained by human-centric factors such as trust, perceived privacy, usability, and the perceived value of concrete use cases (Hofmann et al., 2012; Jurison, 2000).

This section synthesises adoption strategies from three strands of literature: platform and multisided market strategy (chapter 2.2.1), digital identity and eID systems (chapter 2.2.2), and digital wallet and payment systems (chapter 2.2.3). While the platform literature primarily focuses on coordination and launch strategies, the digital identity literature places stronger emphasis on behavioural adoption determinants such as *trust*, *privacy perceptions*, and *institutional legitimacy*. The payment and wallet literature, in turn, contributes empirical insights into incentive design, merchant integration, and cross-side diffusion dynamics. By combining these perspectives, this chapter distinguishes between (1) strategic interventions that wallet providers can deploy and (2) adoption determinants that shape how these interventions can translate into participation decisions. Together they provide a set of strategy "families" that can be applied by wallet providers and orchestrators to stimulate adoption in voluntary, ecosystem-dependent settings such as the EUDIW.

2.2.1 Adoption Strategies from Multi-sided Platform Literature

Solving the chicken-and-egg problem

Platform studies highlight that early-stage multisided platforms must overcome a critical mass hurdle driven by network effects. If participation on one side remains low, the perceived value for the other side diminishes, potentially triggering a self-reinforcing decline in engagement ("*a downward spiral*") (D. Evans & Schmalensee, 2010). Early adoption is therefore primarily a coordination problem.

The platform literature proposes a range of launch strategies designed to overcome this coordination failure. Parker et al. (2016) in their book, described eight strategies for successfully solving the "chicken-and-egg" problem when launching a platform, including *follow-the-rabbit* strategies, *piggybacking*, *seeding*, recruiting *marquee users*, focusing on a *single-side* initially, *producer evangelism*, *big-bang adoption* launch and *micro-market focus* strategies. Rather than representing mutually exclusive approaches, these mechanisms reflect different ways of creating initial interaction density.

Across empirical reviews and student theses on two-sided platforms (Nguyen, 2017; Singh, 2013; Stegellner, 2025), several recurring strategies are mentioned. One group of strategies aims to leverage existing structures. The *piggybacking* strategy, for example, suggests that a new platform should initially build on existing infrastructures, user bases or communities (in our case that could be e.g. building on an incumbent identity solution, a widely used app, or an existing authentication mechanism) to access an already aggregated user base. Closely related are platform *envelopment* and *bundling* approaches, where a new platform attaches itself to an incumbent ecosystem (Stummer et al., 2018).

A second group of strategies focuses on concentrated activation. *Micro-market* strategies recommend launching in narrowly defined geographic, sectoral, or use-case niches where both sides are densely concentrated, so that network effects can form even with small numbers (Parker et al., 2016; Stegellner, 2025). Similarly, recruiting *marquee users* can signal credibility and attract additional participants.

A third approach involves temporarily prioritizing one side of the market (*single-side* or *attract-one-side* strategy). Kao et al. (2020) describe the idea of “*single-player mode*”, where the platform provides standalone value proposition to one group, that is useful even without a fully functioning marketplace. In the digital ID context, this might involve offering secure personal data storage, password replacement, or AV functionality in a way that is useful to users even if very few RPs are on board. Once this single-player value is established, the platform can transition to “*multi-player mode*”, leveraging the accumulated users to attract RPs (Kao et al., 2020).

Stummer et al. (2018) synthesise these insights into six distinct strategies for tackling the chicken-and-egg problem: focusing on a *single target group* initially, *staging* market entry, *subsidising one side*, *envelopment* (bundling with existing platforms), *exclusivity agreements*, and *side-switching* models. Their review makes clear that there is no universally dominant launch strategy; instead, coordination problems are addressed through several tactics in a context-sensitive way.

Asymmetric pricing and subsidization

A main insight of platform economics is that optimal pricing on multi-sided platforms is often structurally asymmetric. D. S. Evans and Schmalensee (2016) argue that platforms frequently subsidize one side, sometimes permanently, by charging zero or even negative prices (for example, rewards or discounts), while recouping costs from the “money side” where willingness to pay is higher. This pricing asymmetry is justified by indirect network effects: additional participation on the subsidised side increases the value of the platform for the money side, which can then be monetized, thereby supporting revenue generation.

In the context of digital ID wallets, this suggests that end-users are likely to be a permanent subsidy side: they are provided with free wallets, simple onboarding, and possibly incentives for using the wallet instead of traditional methods, while RPs bear fees for verification, authentication, or API integration. Unlike short-term seeding mechanisms aimed at initial adoption activation, *asymmetric pricing* can represent a long-term design choice reflecting cross-side value distribution.

Empirical studies of multi-sided platforms further emphasize the importance of tailoring monetisation models to the side that receives the clearest, quantifiable (business) benefits (e.g., reduced fraud, faster onboarding) (de Reuver et al., 2018; Stummer et al., 2018). In regulated ID ecosystems, pricing strategies must therefore balance economic sustainability with adoption incentives across both sides of the market.

Staging and phased roll-out

Beyond initial activation mechanisms, platform implementation is increasingly conceptualized as a multi-stage process. Rather than attempting to scale immediately across all sides and sectors, platform development often follows a deliberate sequencing logic. A recent stage model for multi-sided platforms distinguishes an initial phase focused on achieving interaction stability and critical mass and a subsequent phase of expansion into adjacent networks through *building*, *buying*, or partnering strategies (*strategic alliances*) (Hoskisson & Hoskisson, 2025). Early stages prioritize the stability of core interactions; only after this is secured, it makes sense to scale horizontally into new sectors or add complementary services.

Empirical work on digital ID infrastructures mirrors this logic. The World Bank case study on Singapore’s Singpass and APEX, for instance, emphasises that the government deliberately started with sectors that required high levels of trust and were already under heavy regulation (e.g., public services, banking), and only later expanded progressively to other parts of the economy (World Bank, 2022). This sectoral staging reduced complexity and allowed the orchestrator to learn and iterate before broadening the scope and diffusion.

Platform design and coring

Launch strategies are closely intertwined with platform design choices. de Reuver et al. (2018) point to the idea of “*coring*”, where a platform focuses on solving a key, hard-to-replicate friction at the core of an ecosystem. Rather than attempting to address multiple peripheral problems simultaneously, successful platforms often focus on stabilizing a core interaction that

creates reusable value across contexts. In digital ID ecosystems, this core might be secure, privacy-preserving attribute verification that can be reused across multiple services. By building this core functionality and making it easy for others to integrate it, the platform increases the incentive for ecosystem actors to adopt the wallet on both sides. Coring therefore does not only describe a design principle, but an adoption mechanism: it concentrates value creation in a way that strengthens cross-side participation incentives. At the same time, platform launches show that generic strategies from literature often require significant adaptation in practice, and that onboarding processes, pricing models, and governance structures must be continuously adjusted as the platform learns from early adopters (de Reuver et al., 2018). For wallet providers, this means that adoption strategies should be framed as design hypotheses to be iteratively tested over time, rather than as fixed plans.

2.2.2 Adoption Strategies from Digital Identity and eID Literature

Trust, risk and human-centric cybersecurity

Research on e-government and NDID systems consistently finds that *trust*, *privacy*, *perceived risk*, and *security* are central determinants of adoption. A review of end-user e-government adoption emphasizes that *national culture*, *trust in government*, *perceived system quality*, and *knowledge services* affect citizens' willingness to use digital public services (Jacob et al., 2019). Similarly, Hofmann et al. (2012) identify *trust*, *perceived usefulness*, and *ease of use* as key factors in the acceptance of e-government services across stakeholders.

Focusing specifically on NDID systems, Hilowle et al. (2023) conducted a human-centric cybersecurity review and showed that users' adoption of NDIDs is shaped by a combination of *trust*, *privacy concerns*, *perceived risk*, *usability*, *flexibility*, and *cultural or social influences*. In parallel, research on identity management systems (IdMS) in a blockchain context further shows that behavioural intentions are significantly affected by *perceived usefulness*, *ease of use*, *task-technology fit*, *trust*, *confidence in the internet*, *privacy concerns*, and *perceived cost* (Mohammed, 2021). A correlational thesis study of digital ID adoption in the United States reaches similar conclusions, finding that *perceived institutional trust* is the single strongest predictor of digital ID adoption, alongside *perceived usefulness*, *ease of use*, and *perceived privacy* (Cespiva, 2018). The study further argues that *institutional trust* must be treated as a central pillar for strategies if digital ID systems are to achieve widespread diffusion.

Taken together, this literature converges on a consistent finding: digital ID adoption is strongly conditioned by behavioral and institutional determinants rather than purely technical features. These findings do not describe strategies directly, but rather identify micro-level determinants that influence adoption decisions. For wallet providers, this implies that strategic interventions must address factors such as *perceived trust*, *privacy*, *usability*, and *institutional legitimacy*. In this sense, determinants identified in the digital ID literature represent the behavioral mechanisms through which adoption strategies become effective.

Privacy-by-design and the “privacy adoption paradox”

Studies that examine privacy in eID systems add further nuance to the role of trust and risk in digital ID adoption. A comparative analysis of eID architectures in several EU countries introduces the notion of a “*privacy adoption paradox*”: architectures with objectively stronger privacy guarantees do not necessarily achieve higher adoption rates (Khatchatourov et al., 2015). Adoption is shaped not only by technical privacy properties but also by the way users perceive these protections, trust the institutions involved, and whether they understand the implications of data sharing. The same study highlights two specific adoption barriers in privacy-enhanced eID systems. First, a lack of useful applications (limited meaningful use cases) can suppress adoption even when privacy protection is strong. Second, users may feel uneasy about using a single, official eID card across very different contexts, leading to reluctance to adopt pseudonymous authentication even when it is available (Khatchatourov et al., 2015). Poller et al. (2012) describe similar dynamics in the German eID case, noting a chicken-and-egg problem where service providers hesitate to invest without a user base and citizens do not see enough everyday services to justify adoption. To overcome this, the German government subsidised both sides, funding application pilots for service providers and distributing eID readers free of charge to citizens. This case highlights that privacy protection alone does not drive adoption, complementary measures addressing ecosystem participation are necessary.

Research on engineering *privacy-by-design* into wallet platforms (such as the CREDENTIAL project) demonstrates that translating privacy principles into concrete engineering requirements is complex and often iterative, but it also underscores that visible privacy measures and threat modeling can strengthen perceived trust when properly communicated (Veseli et al., 2019).

Together, these works suggest that privacy-by-design should not be treated as a purely technical compliance exercise. Instead, privacy measures must be embedded within broader adoption strategies that combine strong *use-case availability*, and clear communication about how privacy protections function and why they matter.

Use-case driven strategies and sectoral focus

Case studies of digital ID deployments consistently show that *use-case availability* is a decisive adoption driver. Evidence from digital ID in Chile (OECD, 2019), Estonia’s e-Residency (Tammpuu & Masso, 2019), and Singapore’s Singpass (World Bank, 2022) indicates that users adopt digital ID when it is the easiest or only way to access services that they already value, such as government benefits, tax services, or banking. Rather than promoting digital ID as a standalone product, successful initiatives embed it within high-demand service journeys. The OECD (2019) highlights that successful strategies position digital ID as core infrastructure for broader service transformation and explicitly consider the sectors and applications that will drive adoption among both public administrations and citizens.

The Singpass case is particularly relevant for wallet-like architectures. Singpass and its Myinfo data-sharing component started by targeting sectors that required high levels of trust and were heavily regulated, and then progressively expanded into other sectors. The case study reports significant reductions in onboarding steps (e.g. up to 80% shorter application times and almost 100 fewer “clicks” in some banking journeys) which resulted into higher completion rates and lower acquisition costs for relying parties (World Bank, 2022). This illustrates a *use-case strategy*: identify high-value, high-friction journeys and redesign them around digital ID to make the value of adoption tangible.

At the same time, comparative work on European eID paths shows that different countries have followed very different trajectories, with some opting for software-only solutions and others outsourcing eID management to private actors (Kubicek & Noack, 2010). These variations underline that while use-case prioritization and sectoral staging are recurring strategic patterns, their implementation must be aligned to institutional, regulatory and market contexts.

Usability, UX, and user education

As digital ID wallets provide the primary user interface through which users manage credentials and access services, their *usability* plays a critical role in adoption. A study on user experience (UX) for digital ID wallets concludes that the UX of wallets is still immature and that poor usability can directly undermine trust and willingness to use in practice, even when the underlying technical architecture is secure (Sellung & Kubach, 2023). The findings of this same study identify several recurring challenges. First, the use of technical terminology (e.g., DIDs, credentials) can confuse non-expert users and weaken trust. Second, non-transparent data storage, unclear backup mechanisms, and insufficient recovery options generate uncertainty about control over personal data. Third, structuring wallet interfaces around technical concepts rather than established user mental models creates friction and reduces perceived usability. Conversely, best practices emphasise automatic and clearly explained backup mechanisms, user-friendly but secure authentication, simplistic and responsive design, and accessible tutorials or demo scenarios. Although not all users engage with formal tutorials, clear in-app explanations and transparent communication about how identity data is stored, protected, and recoverable are shown to reduce uncertainty (Sellung & Kubach, 2023). From an adoption perspective, these findings suggest that usability and *user communication strategies* are integral to building perceived trust, control, and competence. Wallet providers must therefore ensure that security and privacy features are not only technically robust but also understandable and aligned with user expectations.

Empirical lessons from Singpass, similarly emphasise prioritising UX throughout the development lifecycle. This includes investing resources to understand user expectations and ensuring accessibility, particularly for vulnerable groups (World Bank, 2022). Together, these findings suggest that usability is not only a technical design concern but an important factor shaping adoption outcomes.

Governance, orchestration and ecosystem strategies

Because ID wallets operate within complex multi-stakeholder ecosystems, adoption is also shaped by governance and orchestration strategies. A recent paper on ID wallets in the context of eIDAS 2.0 distinguishes two government orchestration models: a Government ID-Infrastructure Wallet, which emphasizes public infrastructure and integration, and a Trust ID Wallet Federation, which emphasizes a more competitive, federated setup (Degen & Teubner, 2024). Each model implies different strategies for value creation, tension management, and monetization, but both underscore that clear governance structures are essential for reducing uncertainty and aligning incentives among ecosystem actors.

Similarly, the OECD (2019) analysis on digital ID in Chile introduces a framework that connects national identity infrastructure, policy and governance, technical solutions, adoption factors, and citizen empowerment. This reinforces the view that wallet adoption cannot be treated as a purely technical or market problem; it is an ecosystem governance challenge, where decisions about standards, interoperability, provider roles, and liability shape the willingness of users and RPs to join. In other words, governance structures shape the conditions under which individual adoption determinants (such as trust, perceived risk, expected value) are formed and reinforced.

2.2.3 Adoption Strategies from Digital Wallet and Payment Literature

Although payment wallets differ functionally from ID wallets, both operate as intermediary infrastructures connecting multiple sides of a market (Liezenberg et al., 2019). In both cases, adoption depends on indirect network effects, cross-side participation, perceived trust, and ease of integration. The payment literature therefore provides transferable insights into incentive mechanisms, merchant onboarding, and cross-side diffusion dynamics that are relevant for ID wallet ecosystems.

Incentives, promotions and perceived value

The payment wallet literature provides insight into how digital wallets diffuse among consumers. Studies of digital wallets in Indonesia show that *perceived ease of use*, *trust*, *security*, and *behavioural intention* significantly influence actual usage (Husainah et al., 2023), and emphasise that young users are particularly responsive to usability and security perceptions. Another large-scale study using big data analytics on social media posts about e-wallets finds that users are strongly attracted by *cashback and reward schemes*, and that successful e-wallet business models combine *user-friendly interfaces*, *promotional campaigns*, and *responsive customer service* (Teng & Khong, 2021).

Similarly, Raman and Edward (2018) find that users value *instant payment*, *security*, and *schemes* such as discounts and rewards, and concludes that *interoperability* across wallets, *stronger security*, *broadmer merchant coverage*, and *marketing campaigns* are necessary to grow adoption. These findings suggest that incentive and promotion strategies can play an important role in kick-starting wallet usage, particularly in competitive environments where multiple wallets coexist.

Worldcoin’s wallet adoption study in Thailand similarly points to the importance of *demographic* and *behavioral* factors such as age, income, existing digital wallet possession, usage frequency, and social media engagement in explaining adoption (Kraiwanit et al., 2023). This indicates that targeted marketing and incentive strategies tailored to specific user segments could enhance adoption.

From the perspective of digital ID wallets, these studies imply that even when the core function is not transactional, adoption may benefit from clearly communicated value, temporary incentives, and visible benefits that lower switching costs during early deployment phases.

Merchant/RP adoption, ecosystem constraints and network effects

Payment wallet adoption is not only a consumer issue; merchant (or RP) adoption is equally important for reaching critical mass. The e-wallet big-data study notes that limited merchant acceptance constrains ecosystem growth, whereas competition among bank-led and third-party wallets, as well as regulatory conditions, shapes integration incentives (Teng & Khong, 2021). Low acceptance reduces perceived usefulness for users, thereby weakening cross-side network effects. From an adoption strategy perspective, this underscores the need to support RP integration with technical toolkits, reduce onboarding costs, and demonstrate clear business benefits (such as higher conversion, reduced fraud, or access to new customers). Without a compelling RP value proposition, consumer-side incentives alone are unlikely to sustain adoption.

Research on peer-to-peer payment wallets such as Venmo and WeChat Pay shows how network effects can be socially reinforced. A mixed-methods study shows that social features, including visible transaction feeds and social graphs, accelerate diffusion by signaling widespread usage and enabling interpersonal persuasion (Tang et al., 2019). Interestingly, the mechanisms differ across contexts: U.S. users are more strongly influenced by close ties (“degree effect”), whereas Chinese users are more influenced by widespread community usage (“cluster effect”). The study also shows that while social payment connections rarely become deep social relationships, payment interactions can strengthen existing ties. For digital ID wallets, these insights suggest that RP participation and visible ecosystem uptake contribute to reinforcing user-side value. Even if identity wallets are not designed as social platforms, signaling widespread adoption and enabling smooth integration across services may play a similar role in strengthening cross-side network effects.

2.3 Synthesized Strategy Families & Conceptual Framework

2.3.1 From Individual Mechanisms to Strategy Families

Across the three literature strands, a wide range of adoption-related mechanisms were identified. Some were explicitly described as strategies (e.g., *piggybacking*, *asymmetric pricing*, *seeding*), while others appeared as lessons from case studies (e.g., *subsidized ID reader distribution*, *sectoral roll-out*, *UX simplification*) or as recommendations derived from behavioral adoption research (e.g., *strengthen institutional trust*, *reduce perceived risk*).

Using the analytical criteria defined in the methodology (see chapter 2.1): adoption problem addressed, target actor group, determinants influenced, and contextual conditions, these mechanisms were compared and grouped into higher-level strategy families. This grouping was not based on terminology, but on functional similarity.

- *Piggybacking, envelopment, and bundling* with existing infrastructures were grouped together because they all aim to overcome early coordination failure by leveraging existing user bases. These form part of the **Network Activation** family.
- *Seeding, micro-market focus, and recruiting marquee users* were also included in the **Network Activation** family, as they create concentrated interaction density to trigger early network effects.
- *Asymmetric pricing, subsidizing one side, cashback incentives, and reward schemes* were grouped under **Pricing & Incentive** strategies, since they reduce participation barriers through cost redistribution. The subsidised distribution of eID readers in Germany and onboarding subsidies for service providers were included in this family because they functionally reduce adoption costs on one or both sides.
- *Privacy-by-design implementation, certification mechanisms, institutional endorsement, and clear communication about risk mitigation* were grouped under **Trust & Legitimacy** strategies, as they address perceived institutional trust and perceived risk.
- *UX simplification, automatic backup mechanisms, transparent recovery options, and clear user communication* were grouped under **User-Side Value** strategies, as they increase perceived usefulness and ease of use.
- *Technical toolkits for RPs, API support, integration environments, and demonstrating measurable business benefits* were grouped under **RP-Side Value** strategies, since they reduce integration complexity and increase perceived business value.
- *Sectoral roll-out, phased expansion, and starting in high-trust domains* (e.g., banking, public services in Singpass) were grouped under **Staging & Sequencing** strategies, as they manage ecosystem complexity over time.
- Finally, *government orchestration models, interoperability frameworks, liability structures, and role definitions* within federated ecosystems were grouped under **Governance & Ecosystem Orchestration**, as they define the institutional conditions under which other strategies operate.

This process resulted in seven strategy families summarized in table 1.

Table 1: Literature-derived strategy families and representative mechanisms.

Strategy Family	Representative Strategies Identified in Literature	Adoption Challenge Addressed	Chal- get	Primary Target	Key Determinants Influenced
Governance & Ecosystem Orchestration	Government ID-infrastructure models; federated trust frameworks; interoperability standards; liability rules	Regulatory uncertainty; ecosystem fragmentation		System-level actors	Institutional trust; participation incentives
Trust & Legitimacy	Privacy-by-design implementation; certification; public institutional backing; risk communication	Trust deficit; perceived risk	per-	Users & ecosystem	Perceived institutional trust; perceived risk
User-Side Value	UX simplification; automatic backups; secure but user-friendly authentication; tutorials; high-value use cases	Low perceived usefulness; usability barriers		Users	Perceived usefulness; ease of use
RP-Side Value	API toolkits; sandbox environments; onboarding support; fraud reduction cases; measurable efficiency gains	Integration cost; unclear business case		RPs	Perceived usefulness (RP); perceived cost
Network Activation	Piggybacking; envelopment; seeding; micro-markets; marquee users; single-player mode	Chicken-and-egg coordination failure		Users & RPs	Cross-side perceived usefulness
Pricing & Incentive	Asymmetric pricing; subsidies; cashback; reward schemes; free onboarding	Participation cost barriers		Users & RPs	Perceived cost; participation incentives

Strategy Family	Representative Strategies Identified in Literature	Adoption Challenge Addressed	Chal-enge Addressed	Primary Target	Key Determinants Influenced
Staging & Sequencing	Sectoral roll-out; phased expansion; starting in regulated domains	Scaling	uncertainty; ecosystem complexity	System-level actors	Trust stability; uncertainty reduction

2.3.2 From Strategy Families to a Layered Adoption Framework

While the table classifies the identified strategies according to their functional role and adoption challenge addressed, further comparison revealed that these families operate at different structural levels within the digital ID ecosystem. First, some strategies primarily shape the institutional and regulatory environment in which adoption takes place. Second, other strategies intervene directly at the level of users or RPs. Third, across all strands of literature, adoption is consistently mediated by behavioral determinants, meaning that most strategies influence adoption indirectly through perceptions such as trust, usefulness, risk, or cost.

These observations led to the development of a layered adoption logic:

- **Layer 1: Governance Conditions** (Governance & Ecosystem Orchestration); At the foundational level, governance strategies define the structural conditions of the ecosystem. These include interoperability standards, liability frameworks, certification mechanisms, institutional role allocation, and trust frameworks. Such measures do not directly generate adoption. Rather, they reduce systemic uncertainty, enhance institutional legitimacy, and create predictable rules of participation. In doing so, they shape the conditions under which other strategies can become effective and designed.
- **Layer 2: Strategy Design** (User-Side Value, RP-Side Value, Network Activation, Pricing & Incentive, Staging & Sequencing); At this design level, strategies target specific sides of the market or specific adoption challenges. These include: enhancing user-side value through usability improvements and high-value use cases, strengthening RP-side value through integration support and business case clarity, activating network effects, reducing participation barriers through pricing asymmetries or subsidies, managing ecosystem complexity through staged roll-out. Although these strategies operate directly within the ecosystem, they do not automatically produce adoption. Their effect depends on how they shape user and RP perceptions.
- **Micro-Level Mechanism:** Adoption Determinants; across the literature, participation decisions are consistently linked to a set of recurring behavioral determinants like perceived institutional trust, perceived usefulness, ease of use, perceived risk, perceived cost. These determinants therefore can inform the design of the strategies and, in turn, determine participation decisions. This mediating layer explains why technically advanced or economically rational solutions do not automatically achieve adoption: behavioral perceptions remain decisive.
- **Layer 3: Adoption Decisions;** At this layer, actors make participation choices. Users decide whether to adopt and use the wallet and RPs decide whether to integrate and support it. These decisions are shaped by the determinants described above.
- **Layer 4: Cross-Side Network Effects;** Once adoption begins to grow on one side of the market, indirect network effects reinforce further participation. An increase in user adoption increases value for RPs. An increase in RP participation increases perceived usefulness for users. This cross-side reinforcement can generate self-sustaining growth, but only once critical thresholds are reached.

Figure 3a visualizes the dynamic interaction between strategy domains and the two-sided feedback loop. It highlights how governance, human-centric design, and activation mechanisms collectively shape cross-side value creation. Figure 3b translates this into a structured causal sequence, illustrating the layered mechanism from governance conditions to strategic interventions, behavioral determinants, adoption decisions, and ultimately network effects. Together, the figures move beyond a simple categorization of strategies and provide a structured explanation of how adoption unfolds in multi-sided digital ID ecosystem. Adoption in digital ID wallet ecosystems does not result from isolated interventions, but from the coordinated interaction of user-side value creation, relying-party incentives, and system-level governance mechanisms. First, strategies shaping user trust and perceived value (e.g., usability, meaningful use cases, privacy assurance, institutional legitimacy) directly influence user adoption decisions. However, increased user adoption enhances the attractiveness of the platform for RPs, strengthening cross-side network effects. Second, RP-side value strategies (e.g., integration support, business case clarity) expand the availability of wallet-enabled services. This, in turn, increases perceived usefulness for users, reinforcing user-side adoption. A feedback loop thus emerges in which value creation on one side stimulates adoption on the other. Third, pricing and incentive strategies (e.g., subsidising one side, asymmetric pricing) interact with network-effect stimulation strategies. These mechanisms reduce initial participation barriers and can accelerate the transition from early adoption to critical mass. However, their effectiveness depends on the presence of credible trust and governance arrangements. Finally, platform governance and ecosystem orchestration strategies condition the long-term stability of adoption. Interoperability rules, trust frameworks, and coordination mechanisms reduce uncertainty for both users and RPs, thereby enabling other strategies to function effectively. Taken together, adoption emerges as a systemic and interdependent process. Individual strategies may target specific barriers, but sustained uptake depends on their alignment across user trust formation, cross-side value generation, and ecosystem coordination.

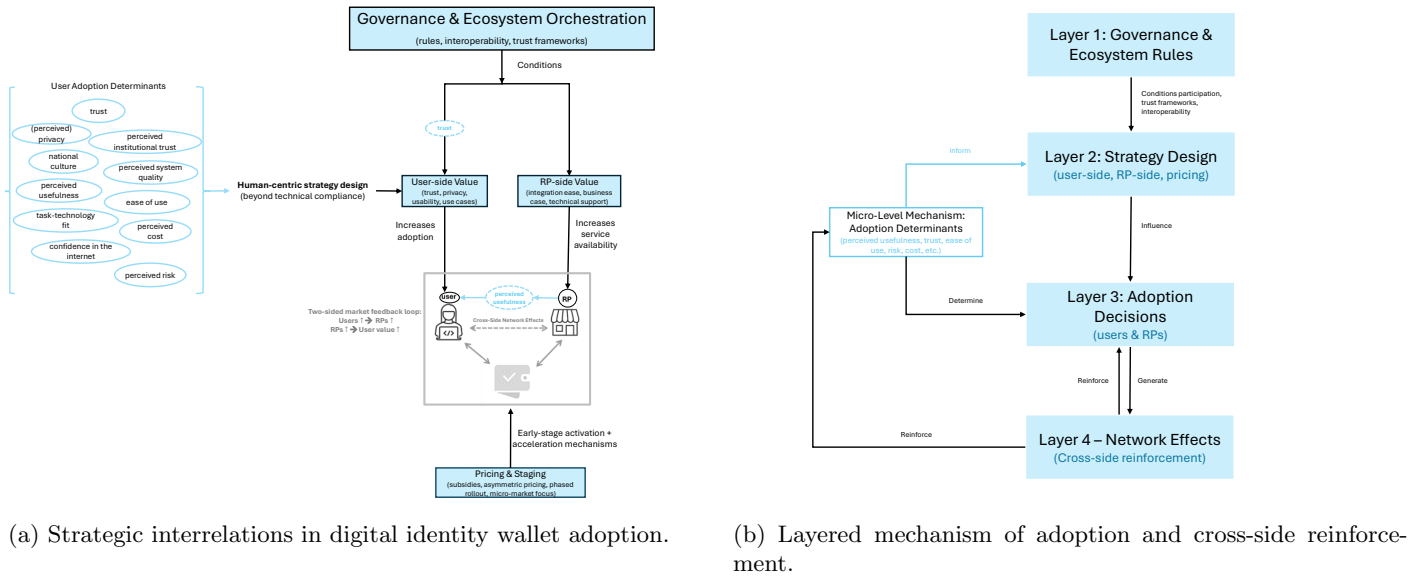


Figure 3: Conceptual framework of adoption strategies for digital identity wallets.

3 Empirical Research Methodology

This section presents the detailed empirical research methodology applied in Stages 2 and 3 of the study. These stages constitute the empirical component of the research and build on the literature-derived framework developed in Stage 1. This chapter details the data sampling, collection, and analysis procedures.

3.1 Stage 2: Expert Interviews

During the second stage of the research, semi-structured expert interviews were conducted, which are the main empirical data source for the study. Semi-structured interviews were selected because they allow for systematic coverage of key adoption themes while retaining the flexibility needed to explore strategic reasoning in depth. This format enables participants to reflect on real-world experiences, explain their reasoning behind strategic decisions, and discuss both successful and unsuccessful adoption approaches.

Two closely related interview guides were developed for this stage. The detailed guides can be found in the appendix 8.3. The first focuses on adoption strategies for digital ID wallets (and digital ID ecosystems more broadly), while the second addresses digital age verification (AV) as a specific use case within ID wallets. The overall structure of both guides was identical, both follow a shared structure, beginning with background and warm-up questions before progressing to strategy formulation, implementation challenges, and lessons learned. The primary differences between the two guides were terminological and emphasis-based rather than structural. For example: questions referring to “digital identity wallets” were reformulated in the AV guide to refer explicitly to “age-verification initiatives”. In the AV version, greater emphasis was placed on distinguishing adoption challenges across user groups and RPs. For instance, the general question “How did you prioritise different adoption challenges?” was specified in the AV guide as: “How did you prioritise adoption challenges for users and for relying parties?”. So, while the conceptual backbone remained the same, the AV guide incorporated more explicit prompts regarding cross-side dynamics. The interview guides served as internal researcher tools to structure the conversations rather than scripts that were read verbatim. While the parts 0-3 and 5 in the guide (opening, consent confirmation, and closing) were read out to ensure ethical and procedural consistency, the main body questions in part 4 were adapted conversationally. Also, they were not shared with participants in advance. In particular, the main interview questions functioned as thematic anchors. Probes and example strategies listed in the guide (e.g., *piggybacking*, *marquee partners*, *micro-market pilots*, *incentives*, *UX redesigns*, *trust-building campaigns*) were not systematically read aloud. Instead, if an interviewee spontaneously mentioned a strategy, the discussion was deepened through follow-up questions. If a key theme had not emerged organically, the interviewer selectively introduced prompts to explore whether similar mechanisms had been considered. Also, the probes were used to clarify or illustrate a question if a participant requested further explanation. The examples were derived from the literature review conducted in Stage 1 and served as a checklist to ensure coverage of literature-identified strategy families. Probes were therefore used flexibly and selectively, depending on the participant’s expertise and the direction of the conversation. Not all probes were used in every interview. This approach ensured comparability across interviews while preserving openness to new or unanticipated strategic insights.

The layered adoption framework developed during Stage 1 (chapter 2.3) also informed the design of the interview guides. The framework conceptualizes digital ID wallet adoption as the result of interacting governance conditions, strategic interventions, and behavioral adoption determinants that ultimately shape participation decisions and cross-side network effects. This conceptual structure was used to define the main thematic areas explored during the interviews. Table 2 illustrates how the conceptual layers

identified in the literature informed the structure of the interview questions. The mapping ensured that the interviews systematically explored governance conditions, strategic interventions, behavioral mechanisms, participation dynamics, and ecosystem-level coordination challenges relevant to wallet adoption.

Table 2: Mapping of the layered conceptual framework to the interview guide

Framework Layer	Interview Guide Sections / Questions	Purpose in Interview Design
Layer 1: Governance & Ecosystem Rules	Warm-up Q2 (organisation’s role in the ecosystem); Section 9 (Q29-31); Section 11 (Dutch Wallet Context); parts of Section 10 (Q35-36)	To examine how interviewees understood the institutional and regulatory environment in which wallet adoption takes place, and how governance arrangements shaped strategic possibilities, barriers, and coordination challenges.
Layer 2: Strategy Design	Section 1 (Q1-3); Section 2 (Q4); Section 4 (Q11-12); Section 5 (Q16); Section 6 (Q20); Section 7 (Q23-25); Section 8 (Q26-28)	To capture the strategic actions and implementation choices used by practitioners to stimulate adoption across different sides of the ecosystem.
Micro-Level Mechanism: Adoption Determinants	Warm-up Q3 (“successful adoption”); Section 3 (Q8-10); Section 4 (Q11-15); Section 7 (Q23-25); Section 8 (Q26-28)	To investigate how practitioners addressed behavioral determinants influencing participation decisions among users and RPs.
Layer 3: Adoption Decisions	Section 2 (Q5-7); Section 4 (Q13-14); Section 5 (Q17-18); Section 10 (Q32-34)	To understand how strategies translated into actual adoption outcomes and which barriers prevented successful uptake.
Layer 4: (Cross-Side) Network Effects	Section 6 (Q19, 21-22)	To examine how practitioners approached ecosystem activation, critical mass thresholds, and cross-side participation dynamics.

It is worth noting that while the layered framework provided the overarching conceptual structure, the interview guide translated these layers into more granular thematic sections in order to make them discussable in practice. This allowed complex adoption dynamics (such as trust-building, RP onboarding, incentive design, and use-case prioritization) to be discussed concretely by practitioners while still maintaining alignment with the theoretical framework.

Prior to the main data collection, a pilot interview was conducted with a consultant specialising in digital identity and payment systems. The pilot interview was used to assess the clarity of questions, the logical flow of the interview, and the overall duration. Insights from the pilot informed minor refinements to question phrasing and ordering, particularly to sharpen the focus on strategic decision-making rather than purely technical implementation details.

Following the first full interview, one additional question was added to the digital ID interview guide. This question asked whether providers had considered implementing AV as a specific use case within their wallet or solution, and if not, what factors influenced that decision. During the first interview, the participant spontaneously referred to AV as a potential wallet use case and shared reflections on its strategic relevance. This indicated that AV was already implicitly connected to broader adoption considerations among providers. However, because the topic had emerged organically rather than through an explicit question, it became clear that subsequent interviews might not address it systematically unless prompted directly. Given that this thesis examines AV as a precursor use case for broader wallet adoption, it was therefore considered methodologically appropriate to include a dedicated question asking whether providers had considered implementing AV and, if not, what factors influenced that decision. The aim was to ensure consistent and explicit coverage of this theme across all subsequent interviews rather than relying on spontaneous mention. The modification was introduced at an early stage of data collection and did not alter the overall structure or thematic orientation of the guide. Instead, it strengthened alignment between the empirical interviews and the central research focus. All subsequent interviews included this question to ensure comparability.

3.1.1 Research Ethics

Prior to data collection, ethical approval for this study was obtained according to the Human Research Ethics Committee (HREC) procedures of Delft University of Technology (Delft University of Technology, 2026). As part of the application process, a detailed Data Management Plan (DMP) was developed outlining procedures for data collection, secure storage, anonymisation, and long-term data handling. In addition, a risk assessment and mitigation plan was completed as required under the HREC checklist. An Informed Consent Form (ICF) template was drafted and reviewed to ensure that participants were fully informed about the aim of the study, that participation is voluntary, and their rights regarding withdrawal and data use. All documentation, including the DMP, risk assessment and ICF, was reviewed and approved by the responsible supervisor and the faculty Data Steward prior to the start of the interviews. As part of the approved data management and risk mitigation procedures, all verified and anonymised

interview transcripts are long-term stored exclusively on TU Delft's secure storage drive. Given the relatively small and highly interconnected expert community in digital ID and AV, it was determined that publishing full anonymised transcripts would carry a residual risk of re-identification, even after removal of direct identifiers. For this reason, full transcripts will not be made publicly available. Only carefully selected and anonymised excerpts (quotes) are used in the thesis and any future research outputs, ensuring that no combination of contextual details could reasonably lead to participant or organisational identification.

3.1.2 Sampling Strategy

The study employed purposive expert sampling, targeting individuals with direct experience in digital identity wallets, trust services, age verification solutions, or related ecosystem roles. The objective of the sampling strategy was not statistical representativeness, but the collection of rich, informed perspectives from actors who have been involved in designing, launching, operating, or orchestrating digital identity initiatives.

Selection of participants was based on the following minimum criteria:

- Direct involvement in a digital identity, wallet, trust service, or AV initiative.
- Strategic or decision-making responsibility (e.g., product lead, strategy advisor, ecosystem manager, regulator, founder) rather than purely technical implementation roles.
- At least several years of professional experience in digital identity, trust services, payments, or adjacent digital infrastructure domains.

This ensured that interviews captured adoption strategies at organizational and ecosystem levels rather than technical implementation details.

The full overview of participants can be seen in the appendix 8.2. In total, 18 expert interviews were conducted, in addition to 1 pilot interview. Out of the 18 interviews, 5 focused specifically on online AV. These included two experts with EU-level experience in AV policy (part of the EU-supported AV Consortium), a representative involved in certification of age assurance schemes, a practitioner with hands-on experience in AV implementation, and an expert involved in an AV wallet initiative in the United Kingdom. Together, these participants provided perspectives spanning policy design, certification and compliance, technical implementation, and market deployment contexts. The remaining 13 interviews focused on digital identity ecosystems more broadly. These included 4 participants from wallet providers, 5 representatives from intermediaries operating as identity brokers, orchestration platforms, or white-label identity solution providers, 2 participants from digital identity solution providers (1 of which represented an unsuccessful initiative), 1 independent consultant with extensive experience advising digital identity programs, and 1 government representative involved in the Dutch national wallet initiative.

The primary geographic focus of the study was the EU, aligning the analysis with eIDAS 2.0 and EUDIW developments. Most participants were based in the Netherlands, with additional participants located in the United Kingdom, Belgium, and Germany. The UK-based participants were included because the United Kingdom represents an advanced regulatory and market context for online age assurance compared to the current EU landscape. Unlike the EU, where the Digital Services Act (DSA) Article 28 (European Commission, 2025e) outlines a requirement for age-appropriate design but has not yet been widely enforced in practice, the UK's Online Safety Act includes enforceable duties on service providers to prevent access to harmful content by children, including through age checks (UK Government, 2025). This means that UK-based providers have been operationalising AV solutions in response to actual regulatory requirements, offering insights into real-world implementation, compliance strategies, and ecosystem effects that are not yet observable in most EU jurisdictions. Furthermore, some UK interviewees brought direct experience or involvement with eIDAS, EUDI, and related discussions, enabling them to bridge perspectives between the UK's regulatory context and ongoing EU developments. Several participants also brought professional experience from digital identity or AV initiatives outside Europe, including work in Asia (notably Japan and India) and Australia. These perspectives were included where they provided relevant comparative insights (e.g., scaling strategies, trust-building mechanisms, governance models).

Recruitment took place through a combination of professional networks, direct outreach and LinkedIn connections. A substantial share of participants were introduced through the professional network of the organisation supporting this research, as well as through the networks of the university supervisors. While this facilitated access to high-level experts, it also implies that part of the sample may reflect overlapping professional ecosystems. However, the digital ID and AV expert community in Europe is relatively small and interconnected, making some degree of network overlap structurally difficult to avoid. In addition, direct outreach via LinkedIn was used, particularly to identify experts specialising in AV. To support this effort, an open call for AV experts was posted on LinkedIn, leveraging the extended professional networks of the supervisors. Through this process, several participants contacted the researcher directly to express interest in participating. In the cases where participants were introduced by third parties or supervisors, all subsequent communication and scheduling were handled exclusively by the researcher. Interviews were arranged using university communication channels and email account in order to comply with institutional ethics, privacy, and data protection requirements. Given the relative scarcity of experts specializing in digital AV (compared to the broader digital ID ecosystem, AV remains a more specialised and emerging domain), targeted outreach was necessary to secure AV-focused participants. Interviews were conducted on a rolling basis, continuing as long as relevant experts were available and willing to participate within the time frame of the study. The extent to which thematic saturation was achieved is assessed reflectively in the discussion chapter (add ref), based on the recurrence and stability of themes across interviews.

It is worth noting that while snowball sampling was actively encouraged during interviews, it resulted in only 1 additional interview. Several factors contributed to this:

- Many suggested contacts had already been included in the sample.

- Some recommended individuals did not respond to outreach.
- Some recommendations pointed toward RPs or adjacent domains (e.g., UK payments initiatives) that would have significantly broadened the scope beyond digital ID wallets and AV, so therefore it was decided to not reach out to them.
- Timing constraints limited extended recruitment cycles.

The limited snowball expansion likely reflects both the relatively small size of the expert population and the tight interconnections within the field. In addition, parts of the data collection period coincided with holiday periods, which may have reduced response rates and limited follow-up availability. Together with the overall timing constraints of the study, these factors likely contributed to the low snowball recruitment effect.

3.1.3 Data Collection

After the date and time for each interview were agreed, a Microsoft Teams calendar invitation was sent to participants, including the meeting link and the ICF (see appendix 8.4). Most interviews lasted approximately 60 minutes (53-75 minutes); one interview was shorter (28 minutes) at the specific request of the participant. This duration was still sufficient to cover the core strategic topics relevant to the study. Interviews were conducted either in person or online, depending on participant location and availability. Four interviews with participants based in the Netherlands were conducted in person at the participants' offices. In these cases, only the researcher joined the Microsoft Teams meeting from their own laptop in order to record the session, while the interview itself took place face to face. During in-person interviews, the camera was switched off and audio recording was enabled. The remaining thirteen interviews were conducted online via Microsoft Teams. For these interviews, video was enabled for both the participant and the researcher, subject to participant consent, and recording was activated.

Each interview began with brief informal rapport-building, followed by confirmation that the participant had received and signed the ICF. Participants were reminded that their participation was voluntary, that they could skip any question or withdraw at any time, and that all interview data would be anonymised.

Interviews followed a semi-structured format. Initial questions focused on participants' backgrounds, roles, and experiences in order to establish contextual understanding. The core of each interview explored strategic objectives, adoption challenges, and the concrete strategies used to address them. Particular attention was paid to two-sided market dynamics, including the interdependence between user adoption and relying-party adoption, the role of trust and privacy considerations, and approaches to solving the chicken-and-egg problem. Later stages of the interviews focused on lessons learned, strategic missteps, and reflections on future risks and opportunities, particularly in relation to the EUDIW ecosystem.

Microsoft Teams' automatic transcription functionality was used to generate initial transcripts for all recorded interviews. These transcripts were subsequently reviewed, corrected where necessary, and anonymised prior to analysis. Detailed procedures for transcript verification and anonymisation are described in the data pre-processing section below.

3.1.4 Data Pre-Processing

All interviews were audio-recorded with explicit participant consent. Microsoft Teams' automatic transcription function was used to generate initial transcripts from the recordings. These auto-generated transcripts were not used directly for analysis. Instead, each recording was manually reviewed in full by the researcher, and the transcripts were corrected and edited to ensure accuracy. This included resolving transcription errors, clarifying unclear passages by re-listening to audio segments, and correcting technical terminology relevant to digital ID and AV contexts.

Following verification, all transcripts were anonymised prior to analysis. Each participant was assigned a unique code. The first two to three letters of the code indicate the participant category:

- WP: Wallet Provider
- DIP: Digital Identity Provider
- DIB: Digital Identity Broker / Intermediary
- GOV: Government Representative
- AV: Age Verification Specialist

These category markers were followed by a random alphanumeric combination (e.g., DIP-9R4K). A full overview of coded participants is provided in the appendix 8.2. In addition, all identifying information was removed or generalised. This included: personal names, organisation names, specific project titles, named partners or clients, location details where necessary and references that could indirectly reveal identity. For example: "*John Doe, Senior Digital Identity Consultant at Innopay, 7 years of work experience*" could be anonymised as "*Interviewee DIP-4SB1, senior consultant in digital identity (5-10 years of professional experience)*" and a reference like "*Worked on the UK Age Verification pilot with major online retailers*" could be generalized as "*Involved in a national age-verification initiative for online platforms*". This anonymisation procedure was explicitly communicated in the ICF (appendix 8.4) to the participants.

Furthermore, during anonymisation, transcripts were also cleaned to remove content not relevant to the research questions. The following elements were removed or summarised:

- Small talk and informal rapport-building exchanges.
- Off-topic conversation unrelated to adoption strategies.
- Personal anecdotes not relevant to the study.

- Stories involving named individuals or organisations.
- Snowballing discussions containing identifying information.

Where content was removed, this was transparently marked in the transcript using brackets such as: [SECTION OMITTED – NOT RELEVANT] or [Identifying details removed] or [...] and visually distinguished in gray color in the working document to preserve transparency in the audit trail. Also, career background sections were selectively reduced where they were not analytically central, while retaining key distinctions regarding role, ecosystem position, and strategic involvement. This process aimed to balance data minimisation with analytical integrity: no strategic arguments, adoption insights, or substantive reflections were removed.

After anonymisation and verification, transcripts were sent to participants for review. Participants were invited to correct inaccuracies, clarify statements and request removal of sensitive quotes. They were asked to respond within two weeks. As stated in the ICF, if no response was received within that period, the transcript was considered approved. Where participants provided clarifications, these were incorporated into the transcript and clearly marked (e.g., [→ Clarification added by participant]) and also in gray colour.

3.1.5 Data Analysis

The aggregated interview data were analyzed using the Gioia methodology (Gioia et al., 2013), which provides a systematic, inductive approach to developing grounded conceptual frameworks from qualitative data. This approach is particularly suitable when the objective is to generate a structured classification of strategic mechanisms while remaining closely anchored in interviewee perspectives. The analysis followed a multi-stage coding process which moved from informant-centric terms to increasingly abstract theoretical categories.

First-Order Coding: Informant-Centric Concepts In the first stage, all verified anonymised transcripts were imported into *Atlas.ti*. The transcripts were then coded sentence-by-sentence to identify distinct statements related to adoption strategies, institutional influences, ecosystem coordination, trust dynamics, and use-case considerations. This stage aimed to preserve the language of the interviewees as much as possible. First-order codes therefore reflected interviewees' own terms and expressions. For example:

- The statement "*The thing with any of that is it's only good if the teeth at the back of it, if it's enforced, and if the penalties are significant, then people will actually follow it rather than breach the law and pay the fines.*" was coded as → "Viewing enforcement as necessary for legislation to drive adoption".
- The remark "*But I would challenge that everybody says that they find it [trust] important, but then in the end, nobody really cares about it.*" was coded as → "Highlighting low salience of trust in user perception".
- The comment "*[...] Because our focus up until now is not really on what we say, low friction, high volume. Those things are, for example, age verifications. We're not not very strong...in those yet, but our strategy is the other way around, so high friction, low volume.*" was coded as "Targeting high-friction, low-frequency use cases".
- The observation "*And I think for relying parties, they want more legislative proof, meaning that we [...] get audited. We're in line with AML regulations, eIDAS 2.0 regulations and we're notified on level high [...]. Users, in my opinion, they don't really care [...]. But for relying parties it is pretty important.*" was coded as → "Highlighting importance of legislative proof for RPs" and "Differing priorities between users and RPs".

Second-Order Themes: Theoretical Abstraction After completion of first-order coding, the full codebook was exported from *Atlas.ti* into *Microsoft Excel*. In this second stage, the first-order concepts were iteratively compared, grouped, and abstracted into second-order themes. This step involved moving from descriptive statements toward theoretically meaningful categories while maintaining empirical grounding. Importantly, codes were not grouped solely based on similar wording, but based on the role they played in the adoption process. In particular, codes were compared in terms of the adoption challenge they addressed (e.g. trust, onboarding friction, cost allocation, regulatory constraints) and the type of strategic mechanism they described. Codes were grouped into themes when they reflected similar ways of addressing a shared adoption problem.

Through constant comparison across interviews, patterns began to emerge around recurring strategic logics. For example:

- Codes related to UX and onboarding (e.g. "Positioning UX as differentiator in competitive wallet markets", "Emphasizing ease of use after onboarding", etc.) and conversion optimization (e.g. "Prioritizing conversion rates in wallet/digital ID solution adoption") were grouped under → "UX & Conversion Optimization", as they all relate to reducing user friction and improving adoption likelihood.
- Codes about cost allocation (e.g. "Placing adoption costs on RPs", "Providing wallet access free of charge to users", etc.) and subsidy structures (e.g. "Subsidizing one market side to stimulate uptake") were grouped into → "Cost Allocation & Cross-Subsidization Strategies", as they all concern how financial incentives and cost distribution are used to stimulate participation.
- Codes about regulatory enforcement intensity (e.g. "Weak or vague regulatory intensity slowing adoption dynamics", "Enforcement viewed as necessary for ecosystem-wide adoption", etc.) and government as accelerator of adoption (e.g. "Viewing regulatory mandates as a way to open one side of the market") were abstracted into → "Leveraging Regulatory Mandates to Stimulate Adoption", as they describe how regulation can be used as an activation mechanism in the absence of voluntary demand.

This iterative abstraction process involved multiple rounds of refinement to ensure conceptual clarity and internal coherence within each theme.

Aggregate Dimensions and Framework Development In the final stage, the second-order themes were further grouped into aggregate dimensions representing broader strategic domains. Rather than identifying isolated tactics, the analysis revealed interdependent strategic domains that wallet providers actively manage when pursuing adoption in the two-sided, platform environment. The themes were not grouped solely based on similarity, but based on the broader coordination challenge they addressed in the adoption process. In particular, second-order themes were clustered when they described complementary mechanisms that together contributed to solving the same underlying adoption problem within the ecosystem. For example:

- Themes like "Leveraging Ownership & Governance Ties for Ecosystem Activation", "Strategic Ecosystem Entry, Targeting, Sequencing" and "Multi-Sided Network Activation & Scaling Dynamics" were grouped into the dimension → "Ecosystem Orchestration & Network Activation", as they all relate to how providers activate, coordinate, and scale participation across different ecosystem actors.
- Themes like "Architectural Trust Engineering" and "Institutional & Brand Legitimacy Transfer" were assigned to the dimension → "Trust & Legitimacy Construction", as they describe complementary mechanisms through which providers increase perceived trust and establish credibility among users and RPs.

The final framework consists of five core strategic domains. In addition, a sixth outer-layer dimension was created ("Structural & Market Context Conditions") in order to capture exogenous factors that shape adoption trajectories (e.g. "Cross-country/cultural variation in digital ID acceptance", "Linking the COVID pandemic to accelerated wallet adoption") but remain largely beyond direct provider control. The resulting data structure is presented in chapter 4.1, which illustrates the progression from first-order informant-centric concepts to second-order themes and aggregate dimensions.

Iterative Refinement and Theoretical Sensitization Although the coding process was inductive and grounded in interviewee language, prior engagement with platform literature and digital ID research informed the analytical lens. In particular, distinctions between user-side and RP-side strategies, governance conditions, and network activation mechanisms were informed by insights from Stage 1 of the research (chapter 2.2-2.3). However, these categories were not imposed during first-order coding. Instead, they emerged during the abstraction stage when comparing empirical themes with literature-derived concepts. The framework therefore reflects an iterative movement between data and theory, consistent with the Gioia methodology, rather than a pre-structured application of existing models.

In addition, it is noted that the first-order coding stage resulted in 436 individual codes. This relatively high number reflects the detailed, sentence-by-sentence coding approach and the fact that interviewees often expressed similar strategic ideas in slightly different ways. During the abstraction phase, overlapping or very similar first-order codes were reviewed and grouped together. In several cases, different interviewees described the same underlying strategic mechanism using different wording. These were consolidated in order to avoid artificial fragmentation of concepts. For the data structure figures presented in the results chapter 4.1, this refinement was necessary to ensure clarity and readability. Conceptually similar first-order codes were therefore grouped under shared labels in the visual representation. The consolidation was limited to semantically overlapping codes and did not remove analytically distinct perspectives. This step ensured that the final data structure reflects conceptual patterns rather than language variation.

Analytical Memos Throughout the data collection, pre-processing and analysis process, analytical interview memos were maintained. Short memos were written immediately after (most) interviews to capture initial impressions, emerging patterns, notable quotes, and contextual observations. Additionally, the memos were updated during transcript verification and throughout the coding process. These notes documented: recurring strategies, early comparisons between interviews, potential links to literature-derived concepts, and reflections on unexpected findings. This process supported iterative interpretation and helped trace the development of second-order themes and aggregate dimensions. Memos were not treated as data themselves but as analytical reflections that informed abstraction and theme refinement.

Theoretical Saturation and Groundedness

Data collection concluded due to practical constraints related to time and access to additional interviewees. However, conceptual saturation was observed at the level of second-order themes and aggregate dimensions. The final three interviews did not generate additional second-order themes or introduce new strategic domains. Instead, they reinforced and elaborated the existing framework.

The four wallet providers generated the most extensive range of first- and second-order concepts, particularly in relation to ecosystem orchestration, incentive alignment, and user enablement. Interviews with brokers and intermediary actors contributed primarily to contextualizing ecosystem dynamics and governance structures. Although participants varied in their market positioning and emphasis, a notable degree of convergence emerged regarding the five strategic domains.

Groundedness was ensured through iterative coding and constant comparison across interviews. Each aggregate dimension is supported by multiple actor types and interview stages, suggesting that the framework reflects recurring cross-case patterns rather than isolated viewpoints.

3.2 Stage 3: AV Use Case

During the coding process, interview segments explicitly referring to age verification (AV) were tagged with an extra code ("AV use case") to allow for focused examination of this specific use case. AV was treated as a voluntary, relatively low-assurance use case within the broader digital ID ecosystem. Rather than developing a separate coding structure for AV, these segments were analyzed within the same first-order and second-order coding framework. This ensured that AV-related insights were interpreted in relation to the broader strategic domains identified across interviews. The AV case therefore functioned as an analytical lens rather than a standalone category. It allowed exploration of how the identified strategic domains apply in a specific use case characterized by rising regulatory pressure and two-sided coordination challenges. This analysis is presented in chapter [5](#).

4 Results: A Multi-Domain Framework of Wallet Adoption Strategies

This study set out to examine what adoption strategies wallet providers could adopt when rolling out digital ID wallets in a two-sided, platform-dependent environment. The findings reveal that adoption is not driven by isolated tactics but by the coordinated management of multiple strategic domains.

Across the interviews, five core strategic domains emerged:

1. Institutional Structuring of Adoption
2. Ecosystem Orchestration & Network Activation
3. User Enablement & Value Proposition Design
4. Economic Architecture & Incentive Alignment
5. Trust & Legitimacy Construction

These domains (aggregate dimensions) operate through distinct but interrelated mechanisms through which wallet providers influence both user-side and RP-side adoption. These strategies operate within broader structural and market context conditions (a 6th dimension), such as cross-border regulatory fragmentation, cultural variation in ID acceptance, and market demand uncertainty. Although providers cannot directly control these exogenous conditions, they must strategically respond to them.

4.1 Strategy Dimensions

4.1.1 Institutional Structuring of Wallet Adoption

Figure 4 presents the data structure underlying the dimension of **Institutional Structuring of Wallet Adoption**. The findings indicate that wallet rollout is deeply embedded in regulatory and political frameworks that shape participation conditions, adoption incentives, and commercialization possibilities. Rather than operating in a purely market-driven environment, providers navigate a highly structured institutional field characterized by compliance requirements, certification regimes, state involvement, and evolving EU-level policy initiatives.

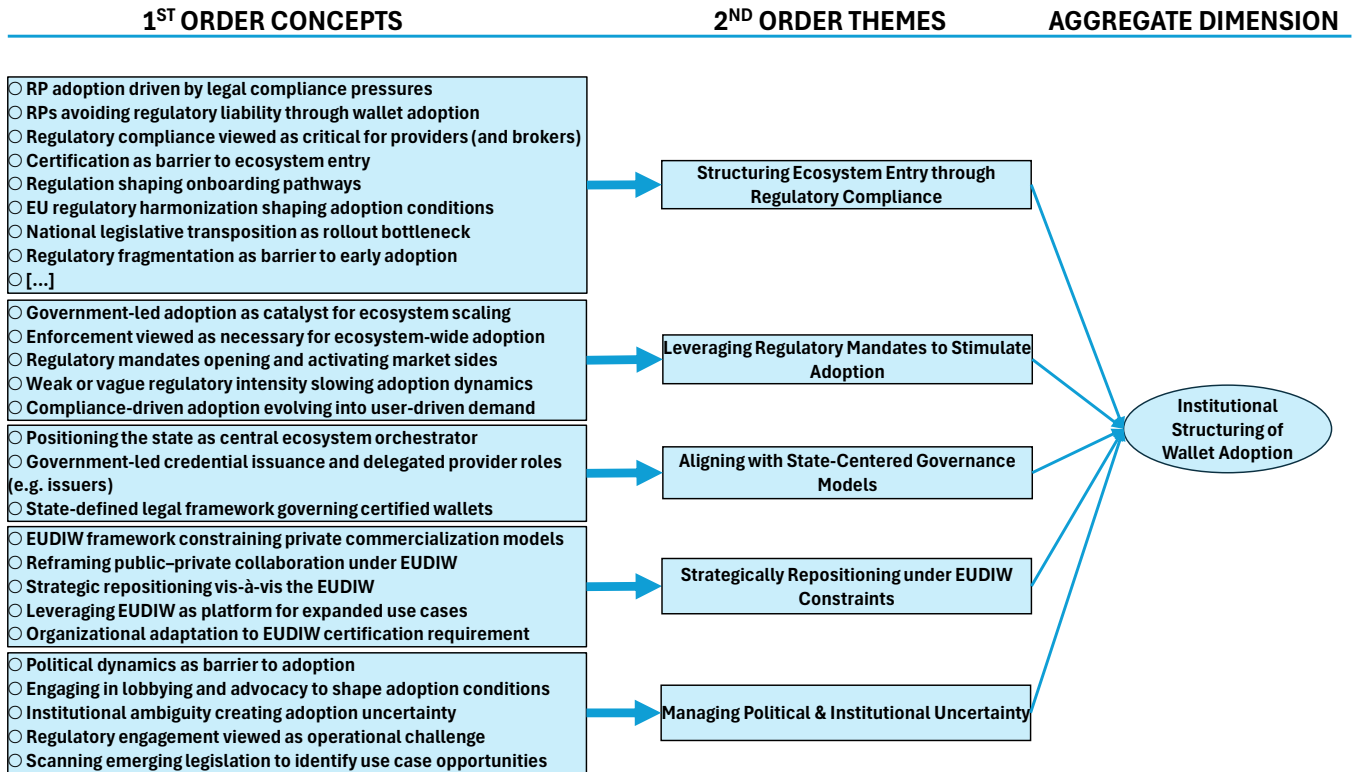


Figure 4: Data structure of strategic dimension 1; Institutional structuring of wallet adoption.

Structuring Ecosystem Entry through Regulatory Compliance The first theme captures how regulation defines the boundaries of ecosystem participation. Interviewees emphasized that RPs decision to adopt wallets is often due to legal compliance pressures and their desire to reduce regulatory liability. As one interviewee noted:

"...what we see is that customers now mainly focus on being compliant. They don't see a lot of opportunities yet to benefit from it, but they mostly are worried about being compliant, especially because many of our customers are in the domain where they have to accept these kind of EU wallets by a certain deadline. So it's more for compliancy than like improving processes or whatever kind of implementation."

In addition, certification schemes and supervisory oversight were described as prerequisites for ecosystem entry. Several providers highlighted that fragmented national transpositions of EU legislation created roll-out bottlenecks, delaying ecosystem scaling. Compliance, therefore, functions not merely as a background condition, but as a mechanism that structures who can enter the ecosystem and under what conditions. Providers must strategically position themselves within these compliance regimes to secure legitimacy and market access.

Leveraging Regulatory Mandates to Stimulate Adoption The second theme highlights the role of regulatory intensity in shaping adoption dynamics. Government-led initiatives and enforcement mechanisms were frequently described as catalysts for ecosystem scaling. Regulatory mandates can open and activate one side of the market by forcing participation from legally obligated actors. At the same time, several participants stressed that legislation alone is insufficient without credible enforcement. One interviewee explained:

"I think the issue that we have or the challenge we face as an identity provider and a trust service provider is that even if there is legislation in place, if there's no enforcement, Dutch companies don't care."

Similarly, another participant described strong resistance to voluntary uptake:

”But still I think companies will only move if they really need to, otherwise they will just not do it. Why would spend the time and energy? I’ve literally had one company say that we’re [...] not unless we need to, we’re not going to do it. It’s also a payment service provider and they are in this business. They’re in the same business. They have strong customer authentication, all kinds of checks and bills they need to do on their clients, literally, they said: I’m not gonna do it until we really need to.”

These statements indicate that adoption decisions are frequently compliance-driven rather than value-driven in early stages. Regulatory mandates therefore function as activation mechanisms in otherwise hesitant markets. In this sense, regulatory enforcement substitutes for missing early-stage network effects. In several cases, interviewees observed that once compliance-driven integration reaches a critical threshold, adoption may gradually shift from obligation-based participation to user-driven demand. This suggests that regulatory pressure can serve as an initial strategic entry lever in two-sided markets characterized by chicken-and-egg dynamics.

Aligning with State-Centered Governance Models The third theme reflects the central role of the state as ecosystem orchestrator. Interviewees described wallet deployment as deeply embedded in public governance structures, including government-led credential issuance, delegated provider roles, and legally defined certification frameworks. Rather than positioning themselves purely as market actors, providers strategically aligned with state-centered governance models. As one provider explained:

”The one thing you still need is a connection with the government. The government has to build the issuing service, that’s the end goal. We’re part of a group of qualified service providers that can provide that issuing service on their behalf, because we’re already working with identity documents.”

Embedding within government-backed systems was described as a way to enhance credibility, access regulated use cases, and reduce institutional uncertainty.

Strategically Repositioning under EUDIW Constraints The introduction of the EUDIW framework was described as a source of institutional disruption. Interviewees highlighted constraints on private commercialization models, expectations of free wallet services, and differences in public-private collaboration. However, perceptions of EUDIW were not uniform. Some participants framed it as a threat to existing business models, particularly for providers positioned primarily as wallet actors. Others viewed it as an opportunity to reposition within the emerging EUDI infrastructure. As one interviewee reflected:

”I think just in general, like the business model is very difficult if you’re only and solely a wallet. So, but yeah, well, I guess we’ll find our way because we play a role in all of the three aspects. We’re active on the issuer side, we have the wallet, and we have connections to businesses. I feel like we have all of the components good at hand and then we’ll see where things take us.”

This statement illustrates the strategic recalibration triggered by EUDIW. Providers described efforts for strategic repositioning. This included reframing their value propositions, internalizing integration capabilities, adapting organizational structures to certification requirements, and identifying new use case opportunities under the evolving framework. Institutional change thus triggered strategic recalibration rather than passive adjustment.

Managing Political & Institutional Uncertainty Finally, the data revealed that political dynamics and regulatory ambiguity create uncertainty that providers must actively manage. Institutional ambiguity regarding accreditation rules, cross-border recognition, and implementation timelines was frequently cited as a source of adoption hesitation. Providers responded by engaging in lobbying and advocacy, maintaining close regulatory engagement, and continuously scanning emerging legislation to anticipate future opportunities and constraints. Political contestation therefore forms part of the institutional terrain that providers strategically navigate during roll-out.

Together, these themes demonstrate that institutional structuring is not merely an external constraint but a strategic domain actively managed by providers. Wallet providers operate within a regulatory architecture that shapes ecosystem entry, adoption intensity, and governance models. However, they actively leverage mandates, align with state models, reposition under regulatory shifts, and navigate political uncertainty to influence roll-out trajectories. Institutional structuring therefore represents a core strategic domain through which providers configure wallet roll-out in a two-sided and highly regulated market environment.

4.1.2 Ecosystem Orchestration & Network Activation

Figure 5 presents the data structure underlying the dimension **Ecosystem Orchestration & Network Activation**. The findings indicate that wallet adoption is not simply a function of user-side design or pricing mechanisms but fundamentally an ecosystem coordination challenge. Providers must activate partners, structure roles, manage intermediation, and sequence market entry to overcome chicken-and-egg dynamics and stimulate network growth.

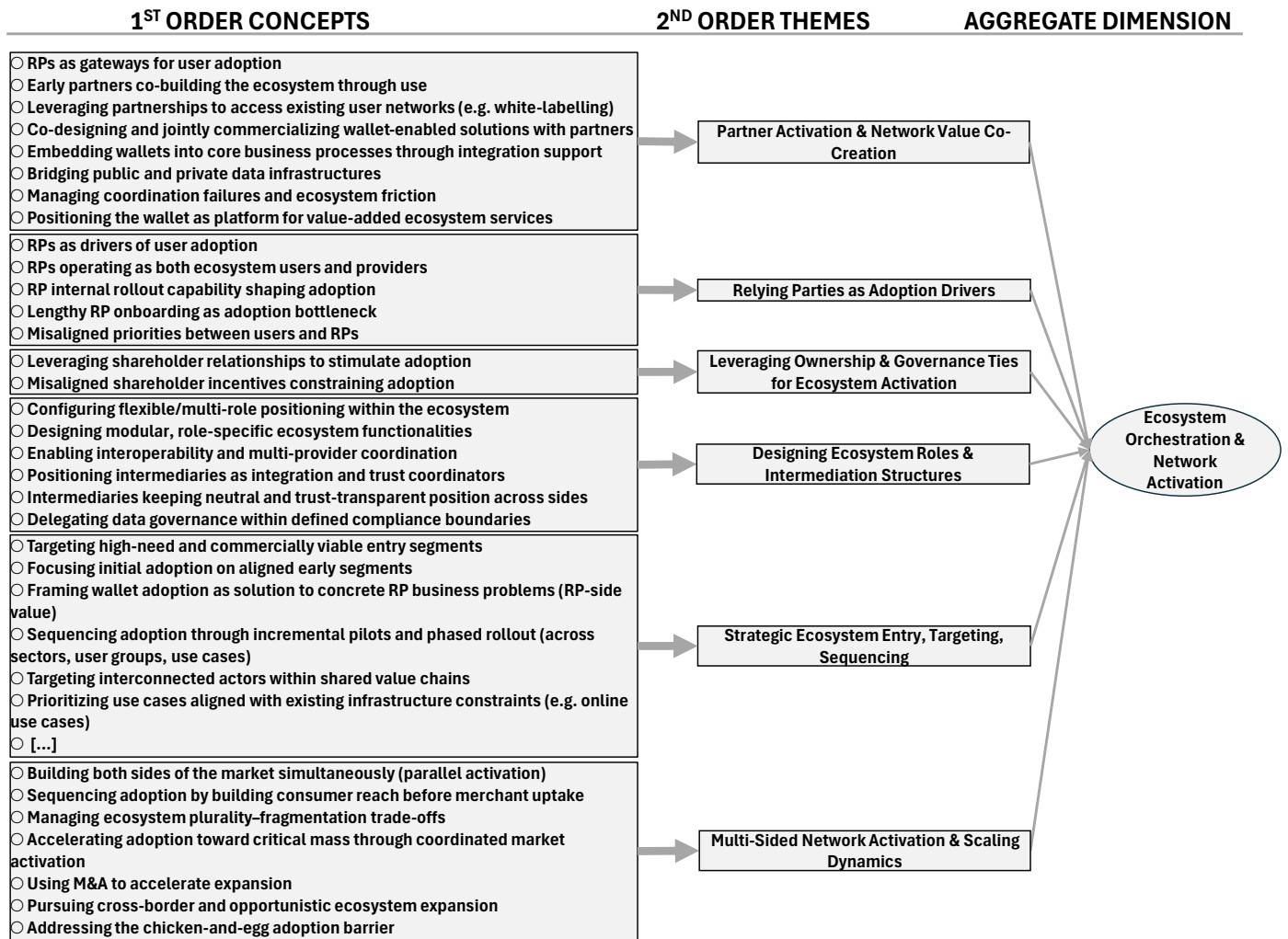


Figure 5: Data structure of strategic dimension 2; Ecosystem orchestration & network activation.

Partner Activation & Network Value Co-Creation This first theme captures the central role of strategic partner activation in driving ecosystem growth. Interviewees emphasized that early partners often co-build the ecosystem by embedding wallet functionality into their services. These integrations serve as validation mechanisms and generate initial transaction flows. Additionally, providers described leveraging partnerships to access existing user networks, including through white-label arrangements and co-branded solutions. In this context, RPs act as gatekeepers to user adoption. As one interviewee explained:

“Because that’s the main focus, the relying party makes the decision to start using a wallet, and in practice you do see that whatever the relying party suggests, the users will take that route.”

This highlights that user adoption is often mediated through RP integration rather than direct consumer pull. Interviewees further noted that providing integration support and technical assistance reduces barriers for partner adoption. In several cases, providers also described bridging public and private data infrastructures and positioning the wallet as a platform for value-added ecosystem services. Therefore, adoption emerges from coordinated value co-creation across ecosystem actors rather than from isolated firm effort.

Relying Parties as Adoption Drivers The second theme highlights the structural role of RPs as ecosystem activation anchors. RPs do not simply adopt the wallet; they control the contexts in which wallet functionality becomes visible and usable. User uptake is therefore frequently mediated through RP integration into core business processes. Beyond integration itself, interviewees emphasised that RP’s internal rollout capability plays a decisive role. Organizational readiness, employee training, and internal communication were repeatedly described as critical adoption determinants. As one provider illustrated:

“We have customers in the same sector with a very similar setup. We sold the same solution to both. One uses it very frequently with strong adoption, whereas the other does not [...] It apparently has a lot to do with internal communication and training employees [...] One organisation simply didn’t manage the rollout well enough [...] So there it is used far less.”

This example demonstrates that adoption success cannot be explained by technical integration alone. Internal change management and operational embedding significantly shape usage outcomes. Moreover, misaligned priorities between users and RPs create coordination challenges. While users may prioritize convenience and seamless experience, RPs often focus on compliance, liability mitigation, and operational efficiency. Providers must therefore align incentives and provide onboarding support to activate the RP side effectively.

Leveraging Ownership & Governance Ties for Ecosystem Activation The third theme is about the strategic use of ownership and governance relationships to stimulate early adoption. In several cases, shareholder relationships provided access to pilot RPs and initial use-case environments. Notably, some shareholders were themselves RPs, which facilitated early experimentation and internal rollout within the organizations. Shareholder-backed RPs were more likely to pilot wallet solutions, providing initial ecosystem traction. This way, governance ties functioned as embedded entry channels into the market. At the same time, interviewees also highlighted that ownership structures could constrain adoption when strategic priorities diverged. In one case, disagreement among shareholders regarding long-term positioning and commercialization direction contributed to the eventual sale of the solution. This illustrates that governance alignment is not automatically stabilizing; it requires ongoing coordination among stakeholders with potentially competing interests.

Governance structures thus operate as both accelerators and constraints, requiring providers to actively manage alignment across ownership stakeholders.

Designing Ecosystem Roles & Intermediation Structures The fourth theme reflects the importance of deliberate ecosystem role design. Providers strategically configure their position within the broader wallet ecosystem, sometimes adopting multi-role positions (issuer, wallet provider, intermediary) and at other times emphasizing modular flexibility. Interviewees highlighted the importance of: designing role-specific functionalities, enabling interoperability across providers, and positioning intermediaries as neutral integration and trust coordinators. Intermediaries were frequently described as actors who reduce ecosystem friction by managing integration complexity and compliance interfaces across sides. Adoption therefore depends not only on technology but on how ecosystem roles and responsibilities are architected.

Strategic Ecosystem Entry, Targeting & Sequencing The fifth theme captures strategic decisions regarding where and how to enter the ecosystem. Rather than pursuing broad launches, providers frequently target high-need and commercially viable segments as entry points. Attempts to build broad ecosystem alliances were often described as unstable and slow-moving. As one participant explained:

"It's very hard to find a coalition. And even if you do, it often dissolves during the setup because there are too many different opinions. What I found more intriguing is the 'atomic network' approach: you start with small use cases, maybe a one-on-one relation between a relying party and an issuer, and solve a very concrete user problem. You do that for one use case, then another, until eventually you can connect the atomics."

This "atomic network" logic reflects a bottom-up activation strategy. Rather than pursuing broad, unfocused launches, providers target narrowly defined, high-need use cases and gradually connect them over time. Incremental pilots and phased roll-outs across sectors, user groups, and use cases were therefore described as mechanisms to build credibility, reduce coordination risk, and demonstrate value before scaling. Also, targeting interconnected actors within shared value chains was suggested as a way to create concentrated activation effects. Additionally, interviewees emphasized that sequencing decisions were often shaped by infrastructural constraints. Offline use cases, for example, may require hardware integration and physical device deployment, significantly increasing coordination complexity. One participant noted:

"If you want to do that [offline use case], you also need the hardware - the ticket scan devices or point-of-sale equipment. So you need a partner that already has that infrastructure. For us, we said: let's first solve the online use case, and only then look at offline use cases."

This illustrates how providers deliberately prioritize digital environments where integration barriers are lower. Sequencing, therefore, is not only a market strategy but also a response to technical and infrastructural constraints.

Multi-Sided Network Activation & Scaling Dynamics The final theme addresses multi-sided scaling dynamics. Providers must actively manage interdependencies between users and RPs, addressing chicken-and-egg barriers through coordinated activation strategies. Some providers pursue parallel activation of both sides of the market, while others sequence adoption by building consumer reach before merchant uptake or vice versa. Managing fragmentation was also a recurring concern. While multiple wallet initiatives may stimulate market experimentation, excessive plurality can slow coordination and delay critical mass formation. Some providers described using mergers, cross-border expansion, or opportunistic partnerships to accelerate scaling once early traction was established. Adoption scaling therefore emerges from deliberate orchestration of network effects rather than organic diffusion alone.

All together, these themes demonstrate that wallet adoption is fundamentally an ecosystem coordination challenge. Providers must activate partners, structure roles, align governance relationships, sequence entry strategically, and manage two-sided network interdependencies. In practice, RP integration functions as the distribution channel for user adoption. Thus, ecosystem orchestration represents a core strategic domain through which providers influence the diffusion and scaling of their digital ID wallets.

4.1.3 User Enablement & Value Proposition Design

Figure 6 presents the data structure underlying the dimension **User Enablement & Value Proposition Design**. The findings indicate that wallet adoption is strongly shaped by how providers design, frame, and operationalize user-side value. Rather than assuming that institutional trust or regulatory compliance alone drive uptake, providers strategically configure usability, perceived convenience, friction levels, and functional benefits to enable adoption in practice. Across the interviews, user adoption was described as highly sensitive to perceived effort, contextual relevance, and immediate utility. Providers therefore actively design the value proposition to align with behavioral adoption logics and everyday usage patterns.

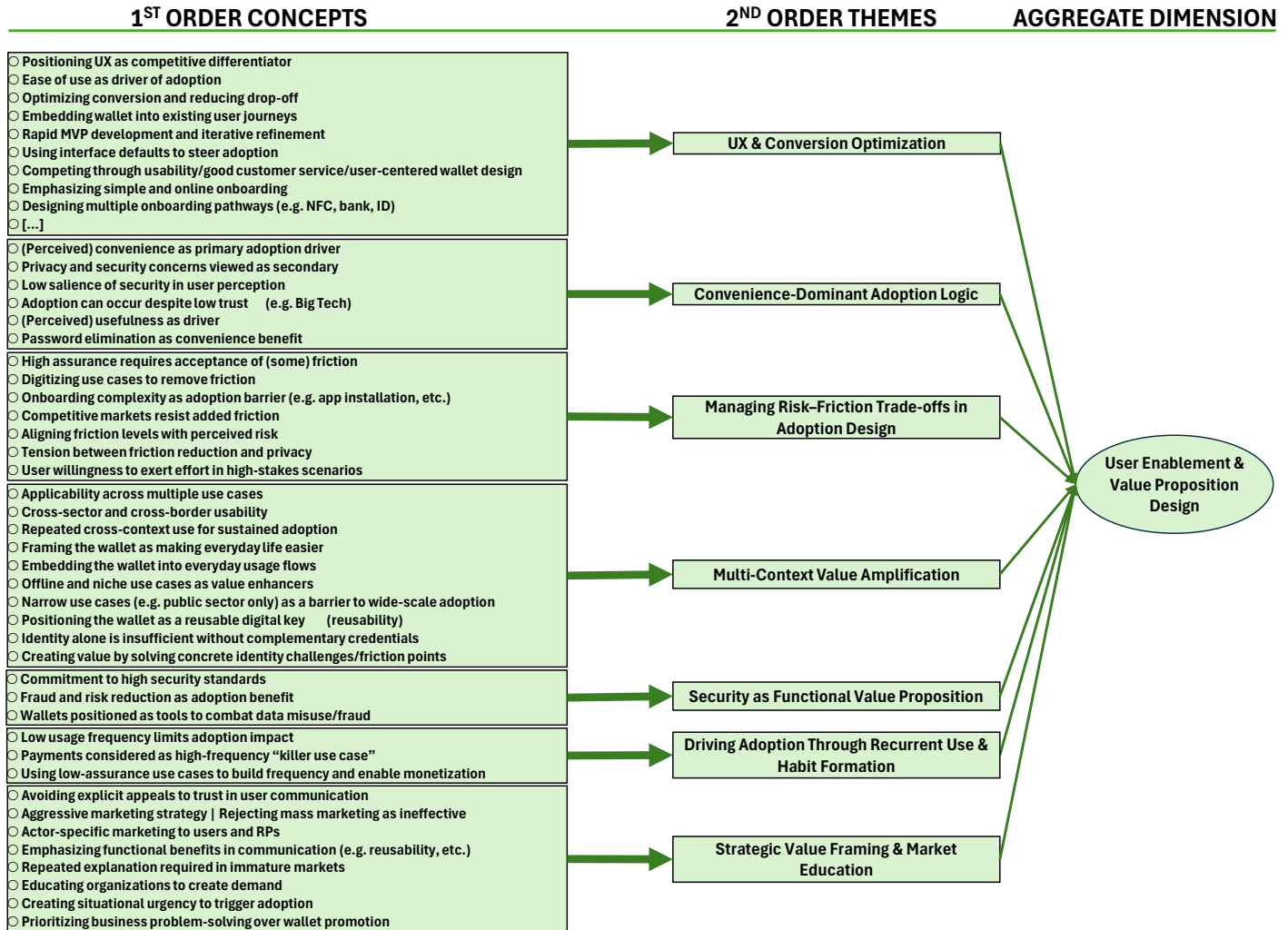


Figure 6: Data structure of strategic dimension 3; User enablement & value proposition design.

UX & Conversion Optimization The first theme captures deliberate efforts to optimize user experience and reduce conversion drop-off. Providers position usability as a competitive differentiator, emphasizing ease of use, intuitive interfaces, and seamless onboarding processes. Strategies include embedding wallets into existing user journeys, minimizing installation steps, and offering multiple onboarding pathways (e.g., via NFC, banking interfaces, or existing digital IDs) to accommodate different user segments. Interface design choices were described as particularly influential in shaping user behavior. One interviewee explained how the positioning of wallet options significantly affected conversion rates:

“In the beginning, the usual process was shown as the main option, and the wallet was just a small alternative underneath: ‘you can also use the wallet, it’s faster.’ But people still chose the main option because it was more visible. At a certain point they switched it up, and that caused a huge change in conversion.”

This illustrates how seemingly minor interface defaults can steer adoption behavior. Rather than abstract value propositions alone, interviewees emphasized that adoption outcomes are often determined by how smoothly and visibly the wallet is integrated at key decision points within user journeys. Also, several interviewees noted that successful wallet platforms adopted rapid MVP development and iterative refinement early on, allowing them to test assumptions, adjust friction points, and improve conversion over time based on user feedback. In contrast, initiatives that delayed market entry or over-engineered solutions before testing often reflected that they wished they had started smaller and iterated earlier:

"Instead of the best product, what I really needed was the cheapest product. As long as it was good enough, yeah."

Convenience-Dominant Adoption Logic The second theme reveals that user adoption frequently follows a convenience-dominant logic. Interviewees consistently indicated that convenience and perceived usefulness outweigh abstract trust considerations in everyday adoption decisions. Privacy and security concerns were often viewed as secondary unless explicitly triggered by a specific incident or in a survey. In several cases, adoption was described as possible even in contexts of limited institutional trust (e.g., major technology platforms), provided that convenience and utility were sufficiently compelling. As one participant put it:

"In the private sector a lot of it comes down to user experience and convenience. Within the industry, we talk a lot about privacy and security. My view is that convenience is king. If something's convenient and attractive to people, their concerns around privacy and security get moved to one side. You see that with things like Facebook, Instagram, Snapchat, TikTok."

Furthermore, password elimination, time savings, and reduced process complexity were highlighted as concrete adoption drivers. This suggests that providers strategically design offerings around behavioral convenience rather than assuming that trust narratives alone generate uptake.

Managing Risk-Friction Trade-offs in Adoption Design The third theme concerns the deliberate calibration of friction levels in relation to perceived risk. High-assurance ID verification processes inherently introduce friction, which can hinder adoption in competitive markets. Providers therefore manage trade-offs between privacy, and ease of use. Interviewees described how users are willing to tolerate friction in high-stakes scenarios (e.g., mortgage applications), but resist it in low-risk or everyday contexts. Strategies, therefore, involve aligning friction levels with user perceived risk, digitizing previously manual steps, and designing assurance pathways that balance security with usability. This way, adoption design becomes an exercise in risk calibration rather than maximizing either security or convenience unilaterally.

Multi-Context Value Amplification The fourth theme captures strategies aimed at expanding the wallet's relevance across multiple contexts. Providers emphasize applicability across sectors, cross-border usability, and integration into everyday use flows to amplify perceived value. Repeated cross-context use reinforces adoption and increases perceived indispensability. Narrow or highly specialized use cases were frequently described as insufficient for large-scale diffusion. As one participant noted:

"If you can use it [the wallet] to log into your government website once a year to fill in your taxes - is that really a success? It might just become that application people remember as: oh yes, that's the app I use once a year."

Similarly, another interviewee reflected on earlier EU initiatives:

"If you look at eIDAS 1.0, the reason why it wasn't particularly successful is because it was purely focused around public sector use cases. People don't interact with government that often in general."

These observations suggest that adoption struggles when wallets are anchored primarily in infrequent, supply-driven interactions. Public-sector use may create baseline legitimacy, but it does not necessarily generate habitual engagement. Rather than positioning the wallet as a single-purpose identity credential, providers frame it as a reusable digital key that supports multiple transactions over time.

In this sense, value amplification emerges not from a single compelling use case, but from cumulative usability across domains and interaction contexts.

Security as Functional Value Proposition Security emerged not only as a compliance requirement but as a functional benefit. Providers position wallets as tools for fraud reduction, misuse prevention, and risk mitigation. Commitment to high security standards and explicit communication of fraud-reduction benefits were described as mechanisms to enhance practical value, particularly for higher-risk transactions. Security therefore becomes part of the value proposition, particularly for RPs, when it addresses concrete pain points, as one wallet provider explained:

"We really try to solve companies' problems, which is fighting fraud. Most of the time there's incomplete data or incorrect data. That's the gap that we try to fill with the concept."

Instead of emphasizing trust rhetorically, providers frame wallet adoption as improving data reliability and reducing business risk. In this sense, security functions as a practical performance benefit rather than simply a legitimacy signal.

Driving Adoption Through Recurrent Use & Habit Formation The sixth theme highlights that sustained adoption depends not only on initial conversion but on usage frequency over time. Several interviewees noted that low-frequency use cases (such as annual tax filings or occasional high-assurance transactions like mortgages) are not sufficient to create long-term impact and user retention. Infrequent interaction limits habit formation and reduces the perceived indispensability of the wallet. Providers therefore seek "frequency anchors": recurring, low-assurance use cases that embed the wallet into everyday routines. Payments were mentioned as a potential high-frequency "killer use case" while other low-assurance verification flows were described as mechanisms to increase interaction density (e.g. AV). Importantly, frequency was also linked to commercialization logic. As one interviewee explained:

"You do need to bring that commercial model in for the low-assurance use cases. In a lot of cases it will be a loss leader, you're earning very little, sometimes nothing, but if you have the right blend, you can earn money in other use cases. By having that frequency, that's where you can sell to the high-assurance use cases because you've built an active user base. And you've created an ecosystem where it becomes worthwhile."

This illustrates a layered adoption strategy: low-assurance, high-frequency interactions may not generate direct revenue but serve as ecosystem builders. They create an active user base that increases the value of higher-assurance, revenue-generating transactions. Recurrent use, therefore, functions both as a behavioral reinforcement mechanism and as a strategic foundation for long-term monetization. Adoption sustainability is not only about trust or usability, but about embedding the wallet into repeat interaction patterns that justify ecosystem investment.

Strategic Value Framing & Market Education The final theme captures how providers strategically frame and communicate the wallet to stimulate adoption. Interviewees repeatedly emphasized that adoption does not occur through abstract appeals to trust or broad mass marketing campaigns. Instead, communication strategies are tailored to specific actor groups and grounded in concrete problem-solving narratives. Several participants noted that explicit trust rhetoric is often ineffective in user communication. Rather than promoting the wallet as "secure" or "privacy-enhancing" providers emphasize tangible functional benefits such as reusability, speed, fraud reduction, or regulatory compliance. Marketing strategies were described as actor-specific. Messaging to RPs focuses on liability reduction, operational efficiency, and fraud mitigation, while user communication highlights convenience and ease of use. Mass marketing was often rejected as inefficient in immature markets where foundational understanding of digital ID remains low. In such contexts, repeated explanation and ecosystem education are required to create demand. Some interviewees stressed the importance of educating organizations first, as user uptake frequently depends on RP integration. Others described creating situational urgency, for example through regulatory change or risk, to trigger adoption. Rather than promoting the wallet as a standalone product, providers frequently frame it as a solution to concrete business or everyday problems. Adoption communication therefore is focused on value realization rather than technological features or abstract trust narratives.

Taken together, these themes show that user adoption is not automatic but must be actively enabled through deliberate value proposition design. Providers strategically configure usability, convenience logic, friction calibration, multi-context applicability, security positioning, habitual integration, and communication framing. This dimension thus represents a core strategic domain through which providers shape behavioral uptake in digital ID wallet ecosystems.

4.1.4 Incentive Alignment & Monetization Architecture

Figure 7 presents the data structure underlying this dimension. The findings demonstrate that wallet adoption in a two-sided ecosystem is fundamentally shaped by how providers design and distribute economic incentives across market participants. Rather than relying solely on intrinsic value or regulatory pressure, providers actively configure pricing structures, cost allocation mechanisms, and monetization models to stimulate uptake on both user and RP sides. Adoption is therefore not only a behavioral or institutional challenge but also an economic coordination problem requiring deliberate incentive alignment.

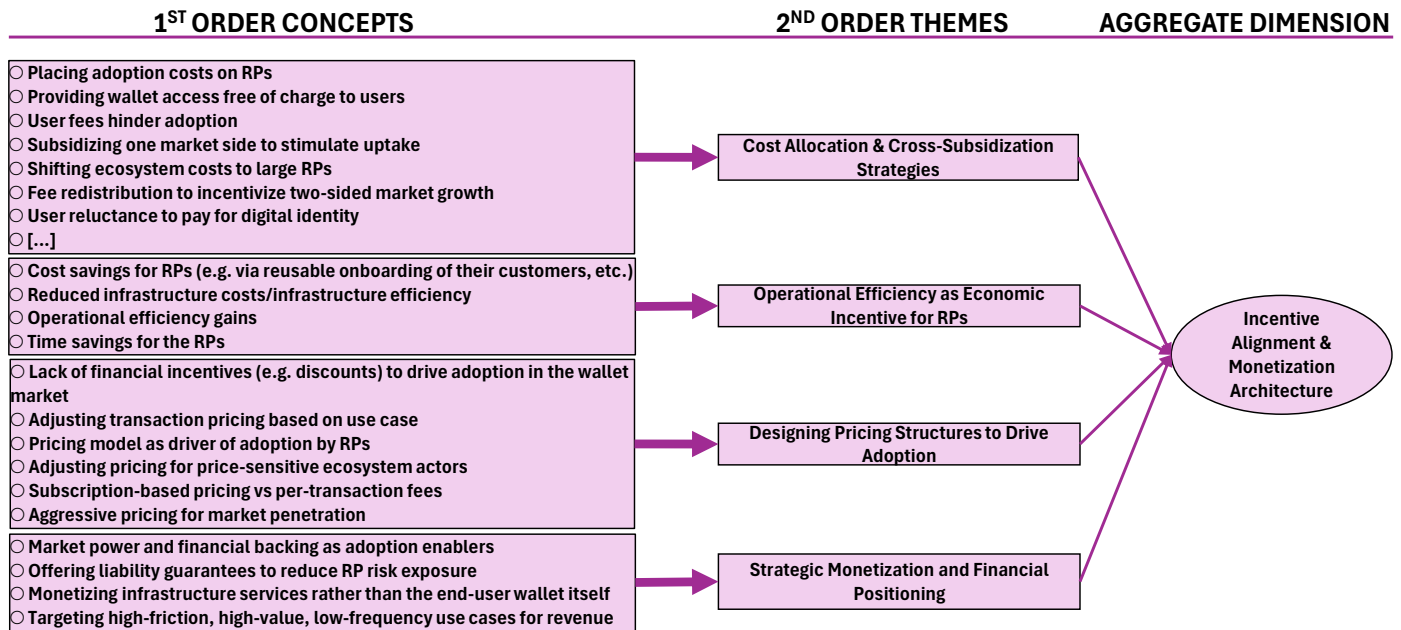


Figure 7: Data structure of strategic dimension 4; Incentive alignment & monetization architecture.

Cost Allocation & Cross-Subsidization Strategies The first theme concerns how providers allocate costs across ecosystem participants. Interviewees frequently emphasized that charging end users directly can significantly hinder adoption, particularly in voluntary ID contexts, where users expect governments or service providers to absorb the costs. As a result, wallet access is typically provided free of charge to users, while costs are shifted to RPs or absorbed strategically by the provider. Several participants described this as a structural feature of identity ecosystems rather than a temporary market entry tactic.

Cross-subsidization strategies, such as subsidizing one market side to stimulate uptake on the other, reflect classical two-sided platform dynamics. Some providers redistribute ecosystem costs internally to incentivize ecosystem growth, while others shift ecosystem costs toward larger or more resource-capable RPs, who have greater operational benefit. These practices indicate that adoption depends on carefully designing who pays and when, rather than assuming symmetric willingness to bear costs across market sides.

Operational Efficiency as Economic Incentive for RPs The second theme captures how operational efficiency serves as a primary economic driver for RP adoption. Interviewees repeatedly framed wallet integration as a mechanism for cost reduction, infrastructure simplification, and time savings. They also highlighted that reusable onboarding processes, reduced manual ID verification, and lower compliance burdens were described as tangible economic benefits. For many RPs, the value proposition lies not in new revenue streams but in operational efficiency gains. As one provider explained:

”So for relying parties using our solution, it’s making the process much faster, and much cheaper and they get much happier clients.”

This suggests that providers strategically position wallets as tools for process streamlining and cost containment, thereby aligning economic incentives with RP organizational priorities.

Designing Pricing Structures to Drive Adoption The third theme reflects the strategic design of pricing models to influence adoption. Providers adjust transaction pricing structures based on use case, price sensitivity, and market maturity.

Subscription-based models, per-transaction fees and aggressive penetration pricing were described as mechanisms to lower entry barriers and stimulate early uptake. Pricing was not treated as a static revenue mechanism but as a dynamic adoption lever. In some cases, pricing adjustments were used to incentivize particular use cases or to encourage specific segments to integrate first. This indicates that pricing architecture plays a strategic role in shaping ecosystem activation patterns and adoption speed.

It is worth noting that, several interviewees noted the absence of direct financial incentives, such as discounts or cashback schemes, to drive adoption in the ID wallet market. Unlike payment ecosystems, where promotional incentives are frequently used to stimulate consumer uptake, identity wallet providers generally do not offer financial rewards to end users. This reflects both structural differences in business models and the perception that ID services are infrastructure rather than transactional consumer products.

Strategic Monetization & Financial Positioning The fourth theme concerns broader monetization strategies and financial positioning. Instead of monetizing the wallet directly at the user level, some providers focus on capturing value through infrastructure services, integration layers, or higher assurance transactions. Market power, financial backing, and liability guarantees were described as mechanisms that reduce perceived risk for RPs and strengthen long-term viability. As one provider commented:

"You need so much market force and you need very strong financial backers if you want to get adoption at scale. So if you're looking at Apple and Google Wallets, it's very simple for them to introduce such a solution and it's frictionless and it's perfect. They have the distribution power."

This statement reflects a broader perception among interviewees that financial credibility and ecosystem reach significantly influence adoption dynamics. Large incumbents can leverage existing user bases, infrastructure, and capital to accelerate adoption, whereas smaller providers must rely more heavily on targeted use cases and strategic partnerships.

These findings suggest that monetization strategy extends beyond pricing models; it involves defining where economic value is captured within the ecosystem and how financial credibility supports adoption.

Taken together, these themes illustrate that adoption in digital ID ecosystems is highly sensitive to incentive alignment across market sides. Providers must strategically configure who pays, who benefits, and how economic value is distributed across actors with asymmetric interests. Incentive Alignment & Monetization Architecture thus represents a core strategic domain through which providers manage two-sided market interdependencies and economically enable wallet adoption.

4.1.5 Trust & Legitimacy Construction

Figure 8 presents the data structure underlying the dimension **Trust & Legitimacy Construction**. While trust is widely discussed in the literature as a central determinant of digital ID adoption, the empirical findings reveal a more nuanced picture. Trust does not uniformly drive adoption across actors. Instead, providers strategically construct credibility, institutional legitimacy, and perceived reliability in ways that vary between users and RPs. Across interviews, multiple participants emphasized that trust is often more decisive for RPs than for end users. While users may adopt based on convenience and functional value, RPs frequently require institutional assurance, compliance guarantees, and reputational credibility before integrating wallet solutions into their services. This dimension captures the mechanisms through which providers strategically build, transfer, engineer, and communicate legitimacy within the ecosystem.

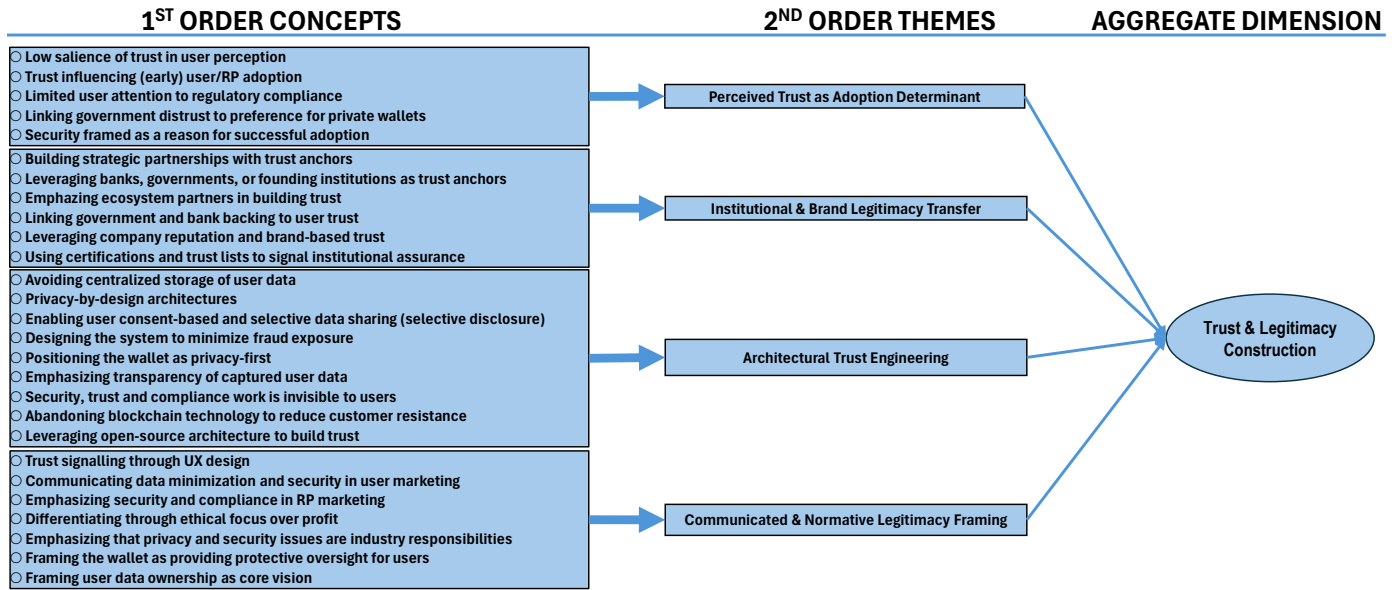


Figure 8: Data structure of strategic dimension 5; Trust & legitimacy construction.

Perceived Trust as Adoption Determinant The first theme reflects how trust operates at the level of perception. Interviewees noted that trust can influence early adoption, particularly in high-stakes or sensitive use cases. However, several participants highlighted that trust often has low salience in everyday user decision-making unless explicitly triggered. Users were frequently described as prioritizing convenience and usefulness over regulatory assurances. Limited attention is paid to compliance status or certification details in routine interactions. In some cases, interviewees highlighted that trust preferences vary across citizens. One government representative noted:

”Citizens vary in their preference and in their trust. Some people trust the government much more than private actors, and for others it’s the other way around. This is why we think it could be beneficial to have both.”

This observation suggests that trust is not uniformly distributed across institutional actors. For certain user segments, public backing may enhance legitimacy, whereas others may express stronger confidence in private providers. From this perspective, ecosystem plurality can function as a mechanism to accommodate heterogeneous trust preferences rather than as a source of fragmentation. At the same time, trust was described as significantly more consequential for RPs. RPs assess legal exposure, liability risks, and reputational implications before adoption. For them, confidence in the provider’s reliability and compliance posture is a prerequisite for integration.

These findings suggest that trust functions asymmetrically across market sides, with RPs acting as primary trust-sensitive actors.

Institutional & Brand Legitimacy Transfer The second theme captures strategies through which providers transfer legitimacy from established institutions and brands. Rather than building trust from scratch, providers leverage associations with recognized actors such as banks, government bodies, or founding institutions. Partnerships with trusted ecosystem actors serve as credibility anchors. Government backing, banking involvement, shareholder structures, and brand reputation were described as signals that reduce perceived uncertainty. Certifications, formal accreditations, and inclusion in trust lists further reinforce institutional legitimacy. For RPs in particular, such signals provide assurance regarding compliance, legal robustness, and operational

reliability. Legitimacy transfer therefore functions as a strategic shortcut to ecosystem credibility. By embedding themselves within recognized institutional structures, providers accelerate ecosystem acceptance and reduce perceived integration risk.

Architectural Trust Engineering The third theme concerns the deliberate design of system architecture to reduce perceived and actual risk. Providers adopt privacy-by-design principles, avoid centralized storage of sensitive user data, and enable consent-based, selective disclosure mechanisms. Technical design choices aim to minimize fraud exposure, reduce linkability, and enhance transparency regarding data processing. In some cases, providers even abandoned certain technologies (e.g., blockchain) when they were perceived to generate user resistance. Open-source architecture and cryptographic safeguards were described as mechanisms to signal robustness and integrity.

Therefore, architectural trust engineering operates at two levels: it substantively reduces exposure to misuse while simultaneously signaling responsible system design. This is particularly relevant in ID ecosystems where misuse concerns can hinder adoption.

Communicated & Normative Legitimacy Framing The final theme highlights the communicative and normative construction of legitimacy. Beyond institutional alignment and architectural safeguards, providers engage in trust signaling through UX design, marketing, and stakeholder communication. Emphasis on data minimization, user control, and protective oversight reinforces perceptions of ethical responsibility. Several interviewees stressed that trust-building efforts often remain invisible to end users unless explicitly communicated. Consequently, providers strategically frame privacy and security as core values, differentiate through ethical positioning, and articulate user ownership of data as a guiding principle.

This communicative dimension complements architectural and institutional mechanisms by shaping how trust is perceived rather than merely how it is structurally embedded.

Taken together, these themes show that trust and legitimacy are not passive background conditions but actively constructed strategic resources. Providers build credibility through institutional alignment, architectural safeguards, and normative framing. Crucially, the findings reveal a market-side asymmetry: trust is structurally decisive for RPs, who evaluate regulatory exposure and operational risk prior to integration, whereas for users it often operates implicitly and becomes salient primarily in high-risk or contested contexts. Trust & Legitimacy Construction thus represents a distinct strategic domain through which providers manage credibility asymmetries and reduce uncertainty within digital ID ecosystems.

4.2 Contextual Dimension

In addition to the five strategic domains identified above, the findings reveal a sixth dimension capturing **Structural & Market Context Conditions**. Unlike the previous domains, these conditions do not represent strategies that providers actively deploy. Instead, they represent exogenous environmental factors that shape the boundaries within which strategic decisions are made. Wallet providers do not control these conditions directly, but they must continuously adapt their roll-out strategies in response to them.

Figure 9 presents the data structure underlying this contextual dimension. Across interviews, five contextual conditions emerged:

1. cross-border fragmentation,
2. market readiness and demand uncertainty,
3. cultural and societal framing of digital ID,
4. organizational risk and entry barriers, and
5. macro-level exogenous shocks.

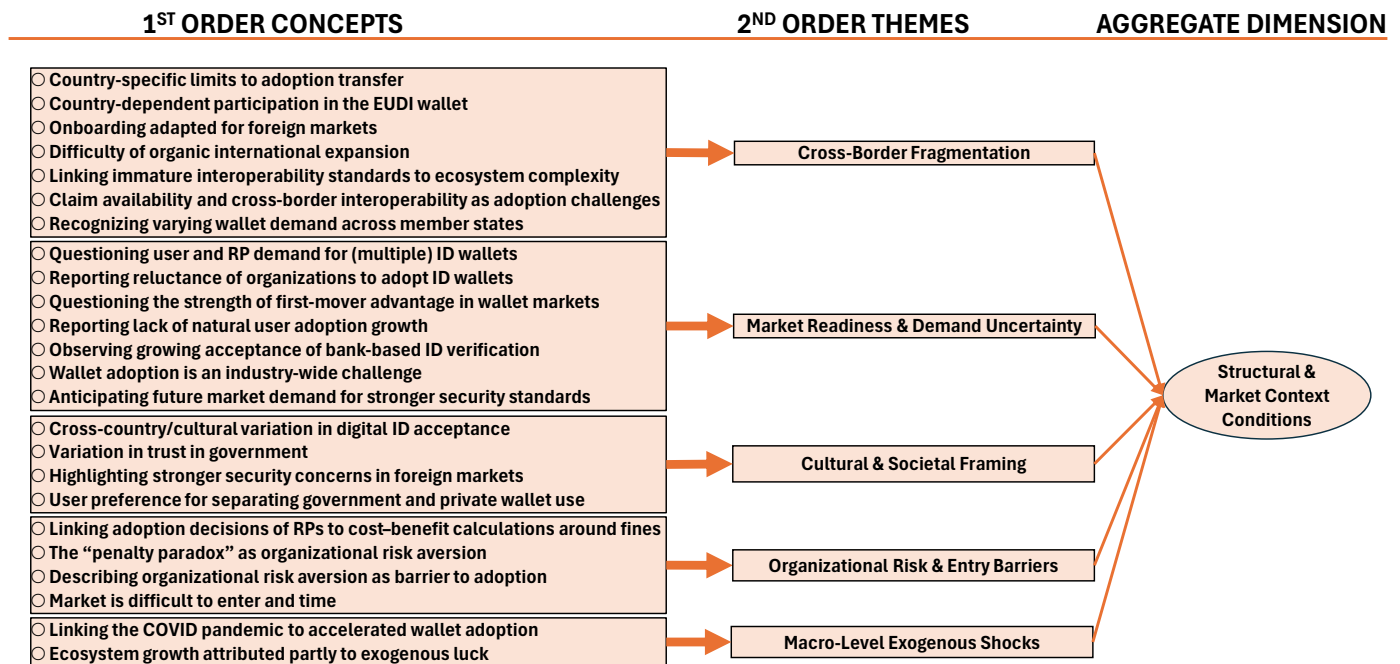


Figure 9: Data structure of dimension 6; Structural & market context conditions.

Cross-Border Fragmentation A first contextual condition concerns fragmentation across national and regulatory environments. Interviewees repeatedly emphasized that wallet adoption dynamics differ substantially across countries due to varying legal frameworks, institutional arrangements, and ecosystem maturity levels. Country-specific regulatory requirements limit the transferability of adoption models from one jurisdiction to another. Participation in initiatives such as the EUDIW varies across member states, and onboarding processes must often be adapted to local institutional conditions. Immature cross-border interoperability standards further increase ecosystem complexity. Moreover, demand levels for wallet solutions differ across markets. Some jurisdictions exhibit stronger institutional readiness and user openness, while others face structural resistance. As a result, international expansion is rarely organic and instead requires deliberate contextual adjustment.

Market Readiness & Demand Uncertainty A second contextual condition relates to uncertainty surrounding actual market demand. Several interviewees questioned both user-side and RP-side willingness to adopt digital ID wallets. Several participants reported limited “natural” user growth, indicating that adoption rarely emerges spontaneously without coordinated activation. Others questioned whether first-mover advantages truly exist in ID wallet markets, given the high regulatory dependency and ecosystem interdependence, which contributes to strategic hesitation. While acceptance of bank-based digital ID solutions is growing in some contexts, broader wallet adoption remains an industry-wide challenge, rather than a single-provider issue. This uncertainty regarding latent demand shapes adoption pacing and increases reliance on coordinated ecosystem activation strategies and regulatory triggers.

Cultural & Societal Framing A third contextual condition reflects cross-country differences in how digital ID is perceived and socially framed. Cultural variation influences acceptance levels, trust in government actors, and attitudes toward private versus public ID provision. In some markets, stronger privacy sensitivity and security concerns shape adoption. In others, users exhibit a preference for separating government-issued credentials from private wallet services. These societal differences influence how wallet initiatives are received and require providers to align their value propositions and legitimacy signals with local expectations.

Organizational Risk & Entry Barriers The fourth contextual condition concerns organizational risk perceptions and structural barriers to entry. Interviewees described RP adoption decisions as influenced by cost-benefit calculations weighing compliance obligations, potential fines, implementation costs, and operational risks. The so-called “penalty paradox” was referenced in some cases, where organizations weigh regulatory sanctions against implementation costs and may delay adoption if perceived enforcement risk is low. More broadly, risk aversion and uncertainty regarding long-term standards create hesitation. Additionally, entering the digital ID provider market itself was described as complex and difficult to time, requiring significant investment and regulatory navigation. These structural entry barriers shape ecosystem composition and competitive dynamics.

Macro-Level Exogenous Shocks Finally, interviewees pointed to macro-level events that influence adoption trajectories independently of firm strategy. The COVID-19 pandemic was frequently cited as accelerating digital service uptake and indirectly benefiting wallet initiatives. In some cases, ecosystem growth was partly attributed to timing, regulatory waves, or favorable external developments rather than deliberate strategy alone. Such exogenous shocks can create windows of opportunity or accelerate latent trends.

Taken together, these contextual conditions illustrate that wallet adoption unfolds within structurally constrained and heterogeneous environments. Providers do not operate in a vacuum; rather, they configure their strategies in response to regulatory fragmentation, uncertain demand, cultural variation, organizational risk perceptions, and external shocks. Structural & Market Context Conditions thus represent an outer contextual layer that shapes, constrains, and enables the strategic domains identified above, influencing the trajectory and pace of wallet adoption across different ecosystem settings.

4.3 Framework

Across the Gioia data structure, wallet adoption did not appear as the outcome of one “best” strategy. Instead, interviewees consistently described adoption as something that emerges when providers configure multiple strategic domains in parallel. Adoption is therefore not a simple product diffusion problem, but a multi-sided coordination challenge that unfolds under institutional constraints. The framework conceptualizes adoption as a configuration of five interdependent strategic domains. Each domain addresses a distinct bottleneck in the adoption process, and strengthening one domain in isolation rarely compensates for weaknesses in the others.

Wallet adoption emerges when providers succeed in:

- navigating and leveraging institutional structures,
- activating RPs and ecosystem partners,
- enabling repeated user use through value proposition design,
- aligning incentives and allocating costs across market sides, and
- constructing trust and legitimacy to reduce perceived RP risk.

These strategic domains form the core logic of wallet adoption, while their configuration must continuously adapt to structural context conditions that shape what is feasible.

What each strategic domain “solves”

The five strategic domains can be understood as answering five practical roll-out questions raised repeatedly by interviewees:

- **Institutional Structuring of Adoption** → Solves: *How do providers navigate regulatory structures and state involvement?*
This domain shows how regulation shapes ecosystem entry, adoption intensity, and permissible roles. Providers actively engage with certification, supervision, and mandates, and reposition strategically under eIDAS/EUDIW constraints.
- **Ecosystem Orchestration & Network Activation** → Solves: *How do providers ensure that RPs and partners embed and promote the wallet?*
This domain reflects the fact that RPs act as gateways for user uptake. Adoption depends on partner activation, sequencing, integration support, and careful role structuring in the fragmented ecosystem.
- **User Enablement & Value Proposition Design** → Solves: *Why should users adopt and keep using the wallet?*
This domain captures how providers reduce friction, optimize conversion, frame convenience-driven value, and expand relevance across contexts (including the “frequency” problem). The underlying mechanism is mainly behavioral: usefulness, ease of use, and habit formation.
- **Incentive Alignment & Monetization Architecture** → Solves: *How are costs and incentives distributed to stimulate two-sided growth?*
This domain captures pricing logics, cross-subsidization, cost allocation decisions, and monetization approaches. Interviewees framed adoption as economically constrained: who pays, when, and for what strongly influences participation.
- **Trust & Legitimacy Construction** → Solves: *How is credibility established; especially for RPs?*
The interviews show that trust is asymmetric: RPs are typically more trust-sensitive than users. Providers therefore build legitimacy through institutional anchors, certification signals, architectural safeguards, and targeted communication.

In addition to the five strategic domains, the data revealed a contextual layer (an "outer ring" inside which adoption strategies are shaped): **Structural & Market Context Conditions**. → Defines: *What constraints shape feasible adoption pathways?* These conditions do not function as strategies themselves, but they shape strategic choice and timing. Interviewees repeatedly highlighted cross-border fragmentation, uncertain demand, cultural variation in trust preferences, organizational risk calculus, and exogenous shocks as factors that affect adoption trajectories and limit straightforward scaling.

How the domains work together

A key empirical insight is that the domains operate as a connected system rather than separate "pillars". Interviewees described recurring dependency chains, as visualized in figure 10. In the figure, institutional structuring defines acceptable roles and certification routes, enabling legitimacy; legitimacy reduces RP risk and supports RP onboarding; RP onboarding creates user exposure through embedded service journeys; and user uptake reinforces RP incentives by making integration worthwhile. Incentive alignment cuts across all domains by shaping who bears costs and how participation is stimulated. Once both sides are activated, cross-side usefulness increases and adoption becomes easier to sustain through reinforcing feedback.

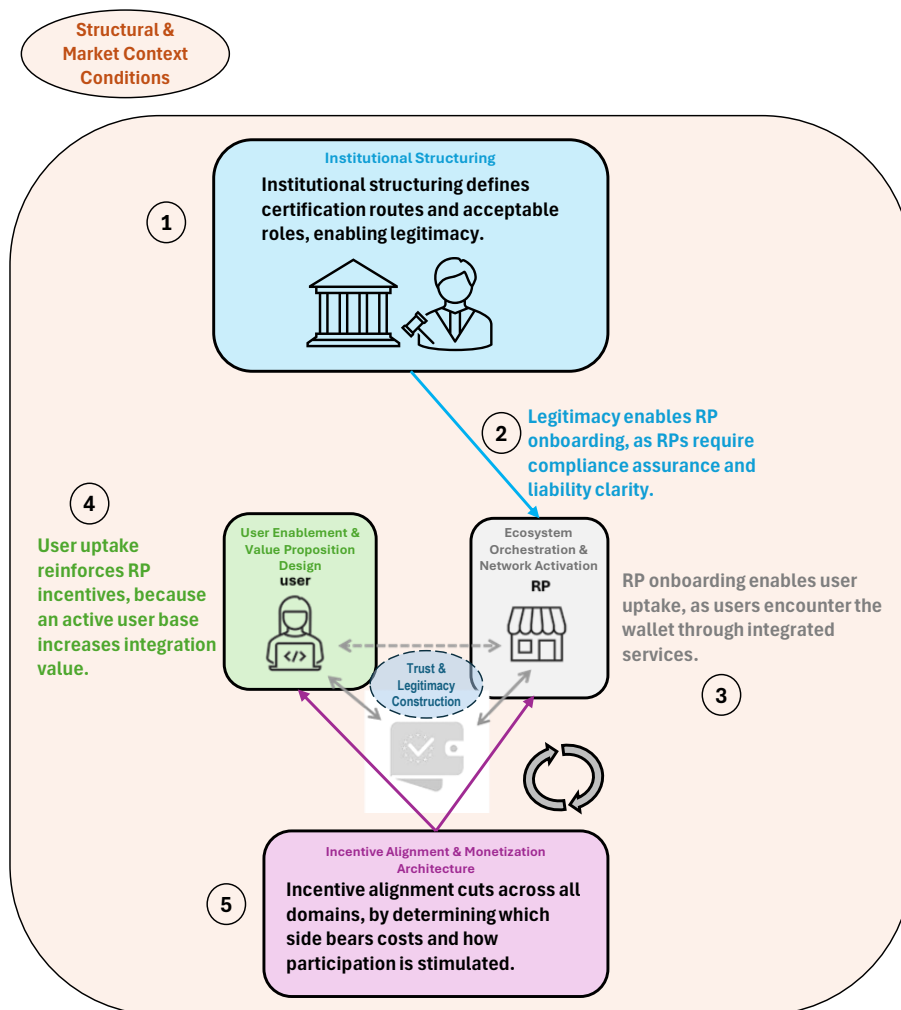


Figure 10: Configurational framework of digital ID wallet adoption illustrating cross-domain dependency chains and reinforcing feedback between RP onboarding and user uptake under structural and market context conditions. Trust & Legitimacy Construction operates primarily as an RP-gating mechanism, reducing compliance and liability concerns that enable ecosystem integration.

Taken together, the grounded framework conceptualizes wallet adoption as follows:

Digital ID wallet adoption emerges when providers configure interdependent mechanisms across institutional structuring, ecosystem orchestration, user enablement, incentive architecture, and trust/legitimacy construction to resolve two-sided coordination under structural constraints.

This framework therefore shifts the focus from “which strategy works best” to **how providers could build a workable configuration** that activates both sides of the market within a regulated ecosystem. While providers often sequence entry through specific use cases and partners, the domains operate in parallel as a configuration rather than a linear stage model.

4.4 Discussion

While the layered framework presented in chapter 2.3 informed the design of the interview guides, the empirical analysis did not impose this structure on the data. Instead, the interviews were analyzed inductively using the Gioia methodology, allowing concepts and strategic mechanisms to emerge directly from practitioners’ perspectives. The resulting multi-domain framework therefore reflects how practitioners describe and configure wallet adoption in practice. The literature review identified seven strategy families and organized them into a layered adoption framework in which governance conditions shape strategy design, which in turn engages behavioral adoption determinants and ultimately affects participation decisions and network effects. While clear parallels exist between the literature derived layers and the empirical domains, the findings reorganize these mechanisms into a configurational set of five strategic domains rather than a sequential layered process. Governance and ecosystem orchestration reappear as institutional structuring; user-side and RP-side value are reworked into the broader domains of user enablement and ecosystem orchestration, respectively; pricing and incentives becomes incentive alignment and monetization; and trust remains central but is broadened into legitimacy construction. The contribution therefore lies in shifting from a layered categorization of mechanisms to a configurational understanding of how adoption strategies are combined in practice.

This discussion relates the empirical findings back to the literature reviewed in chapter 2.2 and shows how the study confirms, refines, and extends existing research on multisided platform strategy, digital ID adoption, and digital wallet ecosystems. Six key theoretical contributions emerge:

From Layered Causality to Configurational Coordination Prior literature conceptualizes digital ID wallet adoption primarily through layered causal mechanisms: governance conditions shape strategy design, which influences behavioral determinants, which in turn drive adoption decisions and network effects. While this layered logic captures important adoption drivers, it implicitly assumes a directional and sequential structure. Prior work on multisided platforms highlights strategies such as seeding, piggybacking, and asymmetric pricing as mechanisms for overcoming chicken-and-egg coordination problems in early-stage platform markets (de Reuver et al., 2018; D. S. Evans & Schmalensee, 2016; Parker et al., 2016). In parallel, research on digital ID and e-government adoption emphasizes behavioral determinants such as perceived usefulness, trust, privacy concerns, and ease of use as key drivers of citizen uptake (Hilowle et al., 2023; Hofmann et al., 2012). The empirical findings refine this perspective by demonstrating that adoption in regulated digital ID ecosystems is better understood as a configurational coordination process. Rather than unfolding in a linear sequence, adoption emerges when providers align multiple interdependent strategic domains in parallel: institutional structuring, ecosystem orchestration, user enablement, incentive architecture, and legitimacy construction. These domains operate as a connected system, in which weaknesses in one domain constrain the effectiveness of others. This shifts the theoretical emphasis from “which strategy works” to how providers configure mutually reinforcing mechanisms under structural constraints. In this sense, the findings integrate insights from platform launch strategy literature and digital identity adoption research by showing how these mechanisms interact simultaneously during ecosystem development.

Regulation as an Activation Mechanism in Two-Sided Markets Platform literature typically treats governance as a background condition that reduces uncertainty and enables participation. In traditional platform markets, early-stage participation is typically stimulated through strategic mechanisms such as subsidies, seeding, marquee users or single-side focus (Parker et al., 2016; Stummer et al., 2018). In contrast, this study shows that in regulated ID ecosystems, institutional structuring can itself function as an active activation mechanism. Specifically, regulatory mandates and enforcement intensity can substitute for missing early-stage network effects. In contexts where voluntary uptake is weak and coordination failure persists, compliance obligations compel RPs to integrate wallet solutions. In this way, regulatory enforcement can perform a role analogous to seeding or subsidy strategies in commercial platforms by triggering initial ecosystem participation. This forced activation can then initiate cross-side reinforcement, triggering user exposure through embedded service journeys. The findings therefore extend two-sided market theory by showing that in highly regulated ecosystems, institutional enforcement does not merely condition adoption in the background; it can actively trigger it. This is particularly important in ID markets, where participation often depends less on spontaneous user demand than on the legal and institutional obligations imposed on organizational actors.

Trust Beyond User Perception: Extending the Behavioral Adoption Lens Existing digital ID literature conceptualizes trust primarily as a user-side behavioral determinant. Studies on e-government and NDID adoption consistently identify perceived institutional trust, perceived risk, privacy concerns, and system quality as central predictors of citizens’ adoption intentions (Hilowle et al., 2023; Hofmann et al., 2012; Jacob et al., 2019). Within this stream, trust operates as a micro-level perception variable influencing willingness to use digital ID services. Research on privacy-by-design further suggests that technical privacy protections only support adoption when they are visible, understandable, and embedded in broader adoption strategies (Khatchatourov et al., 2015; Veseli et al., 2019). The empirical findings of this study extend this perspective by demonstrating that in two-sided digital ID ecosystems, trust also functions as a structural integration requirement for RPs. While users frequently prioritize convenience and perceived usefulness in routine contexts, RPs evaluate wallet solutions through the lens of compliance assurance, liability exposure, reputational risk, and governance alignment. For RPs, institutional legitimacy is not merely a perception variable but a prerequisite

for participation. This finding highlights a previously underexplored asymmetry in digital ID ecosystems, where trust operates simultaneously as a behavioral determinant for users and as an institutional risk-management requirement for organizations.

This shifts the theoretical understanding of trust from a primarily behavioral determinant to a multi-level coordination mechanism. In regulated ecosystems, legitimacy construction does not only influence user attitudes but enables ecosystem integration by reducing institutional and legal uncertainty for organizational actors. Adoption therefore depends not only on fostering user trust but also on establishing credible arrangements that satisfy RP-side risk assessments.

User Value, Use-Case Selection, and RP-Gated Adoption A further contribution concerns the relationship between use-case value, user adoption, and RP-side participation. Prior digital ID literature consistently emphasizes that adoption depends on the availability of meaningful use cases and on embedding digital ID within service journeys users already value (OECD, 2019; Tammpuu & Masso, 2019; World Bank, 2022). Similarly, UX research on digital ID wallets shows that ease of use, clear communication, and alignment with user mental models are critical to adoption in practice (Sellung & Kubach, 2023). In parallel, wallet literature highlights that organizational adoption on the merchant or RP side is necessary for generating user-side value and sustaining cross-side network effects (Teng & Khong, 2021).

The findings confirm these arguments, but also refine them in two ways. First, they suggest that use cases should not be understood merely as static sources of value, but as strategic entry points through which providers attempt to create frequency, reduce friction, and build habitual use. Interviewees described use-case prioritization as a deliberate adoption strategy rather than simply a matter of service availability. Second, the findings show that in many digital ID settings, adoption is strongly RP-gated: users often encounter the wallet only when it is embedded in service access flows created by RPs. This means that user value does not emerge independently from ecosystem participation, but is mediated through RP integration and orchestration. The contribution here is therefore to connect the digital ID literature on meaningful use cases with wallet literature on cross-side activation, showing that user value and RP participation are not separate adoption levers but mutually dependent parts of the same configuration.

Incentive Alignment as a Cross-Domain Coordination Mechanism Pricing and incentive strategies are well documented in platform literature as tools for overcoming participation barriers (D. S. Evans & Schmalensee, 2016). Similarly, research on digital payment wallets shows that adoption can be stimulated through promotional incentives, rewards, and cashback schemes that encourage early consumer usage (Raman & Edward, 2018; Teng & Khong, 2021). However, the findings suggest that in digital ID wallet ecosystems, incentive alignment extends beyond isolated pricing decisions. First, users typically expect ID services to be free, limiting the applicability of direct financial incentives common in payment platforms (e.g. discounts). Second, monetization strategies are constrained by regulatory expectations, particularly under public-sector frameworks such as EUDIW. Third, economic viability often depends on cross-subsidization between low-assurance, high-frequency use cases and high-assurance, revenue-generating transactions. In this context, incentive alignment operates as a cross-domain coordination mechanism: it shapes which actors bear costs, when participation becomes worthwhile, and how strategic domains reinforce one another. This reframes monetization from a tactical lever to a structural element of ecosystem configuration.

Boundary Conditions of Digital ID Adoption Finally, the study contributes by identifying structural boundary conditions that limit straightforward application of general platform growth models to digital ID ecosystems. Comparative studies of NDID infrastructures similarly highlight the importance of institutional context, governance arrangements, and sectoral use cases in shaping adoption trajectories (Kubicek & Noack, 2010; OECD, 2019; World Bank, 2022). The empirical findings strongly support this view. Interviewees repeatedly pointed to cross-border regulatory fragmentation, voluntariness requirements for state-backed wallets, cultural variation in institutional trust, uneven market readiness, and uncertainty regarding enforcement intensity as factors that shape what adoption pathways are feasible.

These contextual conditions constrain feasible strategy configurations and shape the pace and trajectory of adoption. As such, digital ID wallets cannot be understood as purely market-driven platforms. Their adoption logic reflects a hybrid governance environment in which public and private actors co-configure ecosystem development. This introduces important boundary conditions to existing platform and adoption theories, suggesting that highly regulated ID infrastructures require a distinct analytical treatment compared to consumer-oriented digital platforms. More broadly, the findings indicate that adoption strategies in digital ID ecosystems are always embedded in, and limited by, institutional structures that providers cannot fully control.

Taken together, this study re-conceptualizes digital ID wallet adoption as a configurational, institutionally embedded coordination process. By integrating insights from platform strategy, digital ID, e-governance, and digital wallet adoption research, the framework highlights how strategic domains interact to enable ecosystem activation under regulatory constraints. Rather than treating governance, user value, trust, incentives, and network effects as separate variables or sequential stages, the study shows how they are combined in practice as mutually dependent strategic domains. In doing so, the framework extends existing adoption theory and refines platform ecosystem perspectives for regulated digital ID markets.

5 Age Verification (AV) as a Use Case

Age verification (AV) is examined in this study as a focused empirical use case for two reasons. First, AV represents a timely and practically significant challenge within the emerging EUDIW ecosystem. At the EU policy level, AV is actively discussed as a potential early application of digital ID wallets (EUDIWs), as it requires attribute-based verification rather than full ID disclosure. The Digital Services Act (DSA) (European Commission, 2025e) obliges platforms to protect minors but leaves implementation largely to member states, producing uneven market signals across the EU. Meanwhile, a commercial AV market has already emerged in the UK under the Online Safety Act (UK Government, 2025), demonstrating that regulatory enforcement can trigger ecosystem development. These developments make AV a practically relevant and rapidly evolving use case within the digital ID landscape. Second, AV is analytically distinctive because its characteristics represent a particularly demanding test of the strategic domains identified in the framework. Unlike high-assurance ID use cases where user value is more immediate, AV combines weak voluntary user demand, strong RP dependency, regulatory pressure without consistent enforcement, and stigma-related adoption barriers. Together, these conditions create a setting in which the framework's assumptions about voluntary participation, value proposition, and ecosystem coordination are most likely to be challenged. Examining AV therefore allows assessment of how the strategic domains apply when voluntary uptake cannot be assumed and regulatory activation becomes the primary driver of adoption.

5.1 Introduction: AV as a Regulation-Triggered Use Case

AV represents a distinct subset of digital ID use cases characterized by attribute-specific verification, comparatively low assurance requirements, and strong dependence on regulatory enforcement. Unlike full digital ID wallets, which enable multi-context ID transactions and credential portability, AV focuses exclusively on determining whether an individual meets a legally defined age threshold.

Interviewees consistently described AV as narrower in scope and strategically different from high-assurance ID applications. Whereas digital ID infrastructures aim to establish reusable and traceable identity credentials, AV is typically deployed in sector-specific contexts such as online content platforms, gambling services, or alcohol sales. Its emergence is therefore closely tied to regulatory obligations imposed on RPs.

5.2 Regulatory Context: Enforcement as Market Trigger

Across interviews, the development of AV solutions was strongly associated with regulatory enforcement intensity. In the UK, where age assurance obligations have been formalized and enforced through legislation such as the Online Safety Act (UK Government, 2025), a commercial market for age assurance providers has emerged. Interviewees emphasized that legal obligation creates demand on the RP side. One participant explained that, without a mandate, neither users nor platforms have strong incentives to adopt AV:

"Without any mandate...for users it's an extra burden to prove your age if you can instead use the service without proving it. For online services, it's a UX topic and a cost topic. Everything costs to integrate. So there probably needs to be regulatory push to make it happen."

This statement highlights three interrelated barriers to voluntary adoption: user friction, customer UX concerns, and integration costs. In the absence of enforcement, these factors disincentivize implementation. In this context, AV adoption is compliance-driven rather than innovation-driven. Within the EU, however, AV operates under the broader framework of Article 28 of the Digital Services Act (DSA) (European Commission, 2025e), which requires platforms to protect minors but leaves implementation largely to member states. Several interviewees noted that this regulatory ambiguity produces weaker and more uneven market signals. While AV is frequently discussed as a potential precursor use case for the EUDIW (European Commission, 2025a), enforcement mechanisms remain less clearly defined than in the UK. Participants also referenced to the EU-level consortium initiative, which is building a white-label AV application to support member state implementation of DSA obligations. These developments point to a hybrid institutional landscape combining public coordination and private market solutions, though long-term commercial viability remains uncertain in the absence of strict enforcement.

5.3 Conceptual Distinction: Age Assurance (AA) vs. Identity Assurance (IDA)

A central insight emerging from the interview with the expert involved in the age check certification scheme is the explicit conceptual separation between age assurance (AA) and identity assurance (IDA). While these concepts are often conflated in policy debates and media discussions, the interviewee emphasized that they represent fundamentally different problem domains. As the participant explained:

"Age assurance is not the same thing as identity assurance."

AA focuses on determining whether an individual meets an age-related eligibility requirement (e.g., being over 18), without necessarily establishing who that individual is. IDA, by contrast, seeks to confirm a person's full identity in a traceable and legally accountable manner; such as when entering a contract, applying for credit, or purchasing property. The distinction has significant technical and policy implications. According to the interviewee, AA is concerned with answering the question: *"Am I old enough?"*, while IDA answers the question: *"Who am I?"*. The former does not inherently require traceability or full ID disclosure. In fact, the participant noted that in many cases, strong ID linkage may be unnecessary or even undesirable from a privacy perspective.

The interviewee’s distinction aligns with EU-level guidance that refers to AA as mechanisms that determine whether an individual meets the minimum age required to access a particular digital service, such as websites or mobile applications, without necessarily using their full ID.(European Union, 2024b). The interview data strongly reinforced this framing.

5.3.1 Technical Approaches to AA

Building on this conceptual distinction, the interviewee outlined three principal categories of AA methods:

1. **Age Verification (AV)**, which involves determining a person’s date of birth and binding it to the individual. This approach often relies on official ID documents (e.g., passport, driver’s license) or digital ID wallets. Because date of birth is typically stored alongside ID attributes, this method frequently intersects with IDA mechanisms. For example, a user may authenticate via a wallet application and selectively disclose their date of birth. However, the participant emphasized that this is only one method within a much broader landscape.
2. **Age Estimation (AE)**, which relies on analyzing biometric or behavioral features that vary with age, such as facial characteristics, voice, or other physiological markers. These methods do not require access to official ID records but instead generate probabilistic assessments of age. The interviewee described this as conceptually similar to how humans intuitively estimate age based on visual cues, although performed through artificial intelligence and machine learning systems.
3. **Age Inference (AI)**, which draws conclusions about age based on contextual or behavioral information unrelated to date of birth or biometric analysis. For example, holding a credit card, being enrolled in a specific school grade, or possessing a professional license may allow reasonable inferences about age eligibility. Importantly, these methods may not require any formal ID proofing.

As the interviewee stressed, the majority of age assurance techniques do not require full ID verification:

”The vast majority of them don’t require anything about identity as such.”

This observation directly challenges the assumption that AA necessarily depends on digital ID wallets. While wallet-based solutions may facilitate attribute disclosure, AA as a field encompasses a much broader set of technological approaches. The categorization of AA methods described by the interviewee is also reflected in both certification standards and EU-level policy guidance. The ACCS 1:2025 certification framework formally recognizes AV, AE and AI as distinct technical approaches (Age Check Certification Scheme Limited, 2025). Similarly, EU guidance identifies self-declaration, age verification and age estimation as primary mechanisms for determining whether a user meets age-related eligibility requirements. Self-declaration relies on users asserting that they exceed a minimum age threshold (e.g., clicking “I am over 18”), whereas AV involves confirming age through official documentation or electronic identification. AE, in contrast, seeks to approximate age based on biometric, behavioral or contextual indicators, often using techniques based on artificial intelligence (European Union, 2024b). However, AI is not explicitly mentioned in the EU website. While EU guidance lists self-declaration as a distinct method, all interviewees did not consider it a robust AA mechanism, reflecting its limited reliability and low assurance level.

The interviewee further cautioned against reducing the AV debate to a binary between showing a passport and using facial AE. In their words:

”We fall into this trap of thinking it’s only about showing your face or showing your passport...but those are by no means all the ways of doing it.”

According to the participant, over 60 different technological approaches across dozens of providers were identified in their certification work, illustrating the high degree of innovation and diversity within the AA ecosystem. This technological plurality has important implications for wallet providers. If AA can be implemented through a wide range of methods, many of which do not require ID wallets, then AV does not automatically generate structural demand for digital ID infrastructures. Instead, wallets represent one possible implementation pathway among many.

5.4 Strategic Positioning: Standalone Application or Wallet-Integrated Feature?

Beyond regulatory and technical considerations, interviewees highlighted a strategic debate regarding the positioning of AV within the broader digital ID ecosystem. The European Commission frames AV as capable of being implemented either as a standalone application or as a functionality embedded within a multi-purpose digital ID wallet (EUDIW), thereby institutionally legitimizing both architectural pathways (European Commission, 2025a). This debate was shaped not only by architectural considerations, but also by user perception, commercial viability, and regulatory design principles.

Stigma and Multipurpose Framing Several interviewees pointed to a potential stigma associated with standalone AV applications (or AA applications), particularly when linked to socially sensitive use cases such as adult content or gambling. As one participant noted:

”Maybe as a user I don’t want to be seen having that app because then people know what I’m doing.”

This perception creates a reputational barrier to adoption. However, one interviewee (UK based AV solution provider) argued that stigma is mitigated since their application supports multiple use cases beyond age-restricted content:

”The counter to that is that you don’t only use [the solution] to access online adult content. You can use it to open a bank account, prove your right to work, get a new apartment...So it has multiple use cases.”

This suggests that AV providers may strategically incorporate broader ID functionalities to normalize usage and reduce stigma. In this framing, multi-purpose ID functionality serves as a reputational “buffer”, transforming AA from a “special app” into a general-purpose digital credential. This dynamic reveals how AA, while conceptually distinct from IDA, may strategically embed AV within broader digital ID infrastructure.

The two interviewees from the AV Consortium similarly noted that stigma could diminish if AV were required for more common services, such as social media access. One of them even suggested that social media age restrictions could function as a potential “killer use case” for AV (based on user research). If AV were mandated for widely used platforms, such as social networking services, adoption could become normalized at scale. In this scenario, AV would shift from a niche compliance tool to a broadly required digital credential. Participants also pointed out that extending AV to socially accepted offline contexts (such as entering a nightclub or purchasing alcohol from stores) could further reduce stigma by associating the application with routine, legitimate age-restricted activities rather than with socially sensitive online services. However, interviewees emphasized that such normalization would be highly regulation-dependent and subject to the extent of mandated use cases.

Commercial Viability and Market Logic Despite these normalization strategies, several wallet providers questioned the long-term commercial sustainability of standalone AV applications. In markets where enforcement remains uncertain, a single-purpose AV app was viewed as difficult to monetize and maintain. Integrated wallet-based solutions were perceived as potentially more viable because they could leverage existing onboarding processes, credential reuse, and broader ecosystem participation. In this configuration, AV does not constitute an independent product category but rather functions as a low-assurance, habit-forming entry point within a broader digital ID architecture.

Notably, some providers described the Commission’s emphasis on AV, as a potential “marketing strategy” to accelerate adoption of the EUDIW. Consortium representatives, however, rejected this interpretation, arguing that AV was prioritized due to regulatory urgency rather than promotional intent. Additionally, the government-affiliated interviewee emphasized:

”We’re not planning to push a wallet as a technology that has been developed and needs a purpose. The origin of this was that there were challenges for people and organizations that were very difficult to solve without a solid digital identity.”

This reflects a policy framing in which AV is positioned as problem-driven rather than technology-driven. At the same time, the same interviewee highlighted a structural constraint: the EUDIW must remain voluntary under EU legislation. If AV were exclusively available through the wallet, this could effectively force citizens to adopt it. The participant explained:

”You can only ensure the wallet is voluntary when you have a significant alternative. If the Commission pushes this as the only solution...people would be forced to use the wallet, and that is something we do not want.”

This creates an institutional tension. On the one hand, wallet integration enhances normalization and reuse. On the other hand, policy principles require that alternative AV solutions remain available to preserve voluntariness.

5.5 Analytical Synthesis

Taken together, the findings reveal a structural tension at the core of AA development. Conceptually, AA is clearly distinguished from IDA: it concerns attribute-specific eligibility rather than full ID traceability. Technically, it can be implemented through a wide range of methods, many of which do not require integration with digital ID wallets. This plurality challenges the assumption that AA naturally or inevitably leads to broader ID infrastructures.

Yet, strategically, AV frequently becomes entangled with ID integration. The stigma associated with standalone, single-purpose AV applications, particularly when linked to socially sensitive use cases, creates reputational barriers to adoption. In response, providers may incorporate additional ID functionalities, reframing AV as a multi-purpose credential rather than a niche compliance tool. In this sense, ID integration operates as a normalization strategy rather than a technical necessity.

At the same time, interviewees identified large-scale platforms such as social media as potential “killer use cases” capable of normalizing AV through ubiquity. However, such normalization is fundamentally regulation dependent. Without mandated age thresholds, user demand remains weak; and even under regulation, commercialization pathways remain uncertain. Governments may choose to provide or coordinate AV solutions directly, limiting private market opportunities.

Moreover, the requirement that the EUDIW remain voluntary introduces a further institutional constraint. While wallet integration may enhance reuse, habit formation, and ecosystem development, policy principles necessitate the availability of credible alternatives to avoid indirect coercion. This produces a structural duality: AV can be embedded within digital ID infrastructures, yet it must also remain separable from them.

Overall, AA emerges not as a linear precursor to digital ID adoption, but as a contingent and institutionally shaped use case. Its configuration depends on regulatory intensity, public policy objectives, stigma dynamics, and commercial viability considerations. AV therefore occupies an uncertain position within the digital ID ecosystem: conceptually distinct from IDA, technically independent from wallets, yet strategically and institutionally pulled toward integration under specific conditions.

5.6 Applying the Multi-Domain Framework to AV

The preceding analysis examined AV as a regulation-triggered, attribute-specific use case within the broader digital ID ecosystem. In order to address RQ3, this section applies the multi-domain adoption framework (see chapter 4.3) to assess how the strategic domains translate to AV and which AV-specific adjustments wallet providers could consider.

Institutional Structuring: Regulation as Primary Activation Lever

Within the broader wallet ecosystem, institutional structuring shapes ecosystem entry and legitimacy. In the AV case, this domain becomes even more decisive. Unlike high-assurance ID use cases, AV exhibits weak voluntary demand on both user and RP sides. Interviewees consistently described AV adoption as compliance-driven rather than value-driven. In this configuration, regulatory enforcement substitutes for missing early-stage network effects. Where mandates are clear and enforced (e.g., in the UK), commercial AV markets emerge. Where enforcement remains ambiguous (e.g., under evolving DSA interpretations in the EU), adoption signals remain weak. For wallet providers, this implies that AV viability depends heavily on regulatory clarity, enforcement credibility, and alignment with state-backed governance structures. Without institutional activation, other strategic domains (user value, pricing, ecosystem orchestration) struggle to generate uptake.

AV-specific implication: Institutional engagement and regulatory alignment are not supportive strategies; they are prerequisites for AV rollout.

Ecosystem Orchestration: RP-Gated Adoption Dynamics

The framework identifies ecosystem orchestration as central to wallet adoption, with RPs functioning as adoption gateways. The AV case reinforces this dynamic in a particularly pronounced manner; users rarely demand AV proactively. Instead, exposure occurs when RPs embed AV into service access flows. AV adoption is therefore structurally RP-mediated. Furthermore, RPs integrate AV primarily to mitigate liability and comply with legal obligations rather than to enhance user experience. This creates a one-sided activation logic: RP onboarding precedes and conditions user uptake. Unlike broader digital ID applications that may rely on multi-use functionality to attract users directly, AV depends almost entirely on service-side enforcement.

AV-specific implication: Wallet providers must prioritize RP onboarding, integration support, and liability clarity over consumer-facing marketing in early-stage AV rollout.

User Enablement: From Value Proposition to Normalization Strategy

In the general framework, user enablement centers on convenience, usability, and frequency-driven habit formation. In AV, however, user value is structurally weaker. AV introduces friction without offering intrinsic utility beyond regulatory compliance. One interviewee also emphasized that AV may carry a fundamentally negative connotation, as it is often framed as a mechanism for restricting access rather than enabling value. As one participant noted:

"...a lot of the ways people are implementing age verification are around stopping people from doing things. So there's the risk of the negative kind of connotation in that. So while that is fine, at the same time it needs to be seen as an enabler, it needs to be seen as valuable."

This highlights that AV adoption is not only constrained by friction, but also by perception framing. If AV is positioned solely as a control mechanism, user resistance may intensify. Providers therefore face the additional challenge of reframing AV from a restrictive compliance tool to a value-enabling credential. Furthermore, interviewees highlighted stigma and limited perceived usefulness as barriers to voluntary adoption. As a result, providers attempt to normalize AV by embedding it within multi-purpose ID wallets or associating it with socially accepted offline use cases (e.g., entering a nightclub or purchasing alcohol). In this context, ID integration functions as a reputational buffer rather than a technical necessity. Moreover, AV may serve as a low-assurance, high-frequency entry point when embedded in broader wallet infrastructures. As a standalone application, however, it lacks sufficient user-side pull to generate sustained engagement.

AV-specific implication: For wallet providers, AV should not be framed as a standalone value proposition but as either a compliance service for RPs or a habit-forming feature within a broader wallet ecosystem.

Incentive Alignment: Limited Monetization and Cross-Subsidization Logic

The general framework emphasizes incentive alignment and cost allocation as cross-domain coordination mechanisms. In AV, incentive constraints are particularly pronounced. Users are unlikely to pay for AV. RPs may integrate AV only when legally required. Furthermore, regulatory expectations under EUDIW and public-sector involvement may limit direct monetization opportunities. As several interviewees noted, standalone AV solutions face uncertain commercial sustainability in markets with weak enforcement. Integration into broader wallets may allow cross-subsidization, where low-assurance AV transactions support ecosystem density that increases the viability of higher-assurance services.

AV-specific implication: AV is unlikely to function as a self-sustaining commercial product in voluntary markets. Providers must evaluate whether AV serves as a strategic ecosystem builder rather than a primary revenue generator.

Trust & Legitimacy: Dual-Level Trust Construction in AV

The framework distinguishes between user-side behavioral determinants and RP-side legitimacy requirements. The AV case suggests that trust operates at both levels, though in distinct forms. On the user side, trust concerns center on privacy reassurance and

non-traceability. Interviewees emphasized that users may fear being tracked or stigmatized when using AV applications. As one provider explained, certified AV providers operate under a “double-blind” model:

“We don’t have a record of how many adult content sites you’ve visited versus how many bank accounts you’ve opened... We can prove that we can’t see that data.”

Here, trust is constructed through architectural design (data minimization, non-linkability) and verifiable certification. Trust signaling therefore focuses on reassuring users about what is not visible or stored, and clarifying which data is shared with whom. In this sense, privacy-by-design becomes a visible trust mechanism rather than a purely technical compliance feature. At the institutional level, trust operates as legitimacy assurance for RPs and ecosystem actors. Participation depends on inclusion within formally recognized trust frameworks, such as EU-level trusted lists and certification regimes. As one interviewee noted, AV providers must be placed on a member-state-backed trusted list, making trust contingent on formal institutional recognition. Thus, in the AV context, trust is neither purely behavioral nor purely institutional. It is constructed through a dual mechanism: user-level privacy reassurance and system-level compliance legitimacy. Regulatory structures shape both dimensions. At the same time, the requirement that the EUDIW remain voluntary introduces a structural boundary condition. If AV were exclusively delivered through the wallet, voluntariness principles could be undermined. Policymakers must therefore preserve credible alternatives, reinforcing that legitimacy in AV depends not only on privacy guarantees but also on institutional design choices.

AV-specific implication: Trust construction in AV requires both visible privacy assurances for users and formal certification/recognition mechanisms for RPs. Providers must signal non-traceability while simultaneously embedding themselves within recognized governance frameworks.

Overall Assessment: AV as a Stress Test of the Framework

Applying the multi-domain framework to AV reveals that the configurational logic holds, but with altered weightings across domains.

Institutional structuring becomes the dominant activation mechanism, as regulatory clarity and enforcement substitute for weak voluntary demand. Ecosystem orchestration is heavily RP-gated, with RPs acting as the decisive integration anchors through which user exposure occurs. User enablement shifts from intrinsic value creation toward normalization and stigma management, particularly when AV is embedded within broader ID infrastructures. Incentive alignment is constrained by limited willingness to pay and uncertain commercialization pathways, often requiring cross-subsidization or ecosystem embedding. Trust construction operates at two levels: visible privacy reassurance for users and formal institutional legitimacy for RPs.

Taken together, AV illustrates that digital ID adoption strategies are highly contingent on use-case characteristics. Unlike high-assurance, value-rich ID applications, AV represents a regulation-triggered, low-assurance, platform-dependent use case with limited intrinsic user pull. Its viability depends on enforcement intensity, governance credibility, stigma mitigation, and its integration within a broader ecosystem configuration. In this sense, AV should not be understood as an automatic precursor to broader wallet adoption. Rather, it functions as a conditional entry point whose strategic value depends on how effectively providers align regulatory positioning, RP integration, trust signaling, and incentive structures within the wider digital ID architecture.

5.7 Summary

This chapter examined AV as a strategically relevant use case within the emerging EUDIW ecosystem. The findings show that AV is not simply a narrower version of digital ID, nor an automatic precursor to broader wallet adoption. Conceptually, AA is distinct from full IDA because it focuses on attribute-specific eligibility rather than full ID traceability. Technically, it can be implemented through multiple approaches, many of which do not require a digital ID wallet.

At the same time, the analysis shows that AV (AA using ID) can become strategically connected to wallet adoption under specific conditions. In particular, AV becomes relevant to the EUDIW when regulatory enforcement creates RP demand, when wallet integration helps normalize use and reduce stigma, and when providers use AV as a low-assurance entry point within a broader ID ecosystem. Its relevance therefore does not lie in technical necessity, but in its potential institutional and strategic role as a regulation-triggered, ecosystem-activating use case.

Applying the multi-domain framework to AV demonstrates two things. First, the configurational logic of the framework holds across use cases with different characteristics. All five strategic domains remain relevant in the AV context, confirming that the framework is not limited to high-assurance, high-value ID applications. Second, and more importantly, the relative weight of each domain shifts significantly depending on use-case conditions. In AV, institutional structuring becomes the dominant activation mechanism because regulatory enforcement substitutes for missing voluntary demand. Ecosystem orchestration is almost entirely RP-driven, as users rarely seek out AV independently. User enablement shifts from creating intrinsic value toward managing stigma and normalizing use. Incentive alignment is constrained by limited willingness to pay and uncertain commercialization pathways. Trust construction operates simultaneously at the user level through privacy reassurance and at the RP level through certification. Together, these findings show that adoption strategies in digital ID ecosystems cannot be treated as universal prescriptions. The same strategic domains apply across use cases, but their configuration (which domains take priority, how they interact, and what constraints they operate under) depends on the specific regulatory, commercial, and institutional conditions of each use case. By examining AV as a focused use case, this chapter has demonstrated that the multi-domain framework can be applied diagnostically to derive context-specific strategic priorities.

6 Extended Discussion

While the previous chapters developed and applied the multi-domain framework of digital ID wallet adoption, this chapter takes a step back to reflect on broader strategic tensions and implications that emerge from the findings. In particular, it discusses several recurring strategic tensions highlighted by interviewees that extend beyond the immediate empirical results and require further reflection. These include questions around user incentivization and the relationship between identity and payment ecosystems. In addition, the chapter examines how the framework applies to government-issued digital ID wallets and further discusses the boundary conditions under which it holds. Together, these reflections position the findings within wider debates on platform strategy, governance, and digital ID infrastructure development.

6.1 The Debate in Digital Identity Ecosystems: Should the user be free?

One recurring strategic tension concerns whether end users should directly pay for digital ID wallets. The majority of ID providers interviewed expressed the view that users are unlikely to accept direct payment for ID services. Several participants argued that users expect digital ID to be either government-facilitated or indirectly financed, rather than treated as a consumer product. As one interviewee noted, users are unlikely to “*suddenly start paying for an identity*”, particularly in contexts where digital ID functions as foundational public infrastructure rather than as an optional consumer-facing service.

In practice, costs may already be indirectly borne by users; either through RP fees embedded in services (e.g., financial onboarding processes) or through taxes in government-led models (public wallets). However, this indirect cost structure is typically invisible to users.

Interestingly, while most providers rejected direct user charging models in the current market context, some acknowledged that from a business-model perspective, a “user-pays” structure would represent a “purer” business model. One interviewee argued that if wallets were funded directly by users (similar to password managers) providers would serve user interests more exclusively rather than prioritizing RP demands. This framing introduces a normative and governance dimension: direct user payment could theoretically align incentives more closely with privacy and user sovereignty goals.

At the same time, one case mentioned during interviews involved an RP that passed ID transaction costs directly to users. Although this initiative was ultimately discontinued, ID transaction volumes reportedly increased during its operation. It remains unclear whether this was driven by lack of alternative identification options, the specific use case, or contextual market conditions. This suggests that direct user charging should not be dismissed categorically and may depend strongly on use-case friction, regulatory context, and market structure.

The question of whether users should directly pay for ID services therefore remains open and may evolve as digital ID becomes more normalized in society. Future research could examine willingness-to-pay dynamics, incentive alignment effects, and long-term sustainability of alternative funding models.

6.2 Identity and Payments: Two Distinct Strategic Debates

6.2.1 Payments as a Use Case within Digital Identity Wallets

Several interviewees described payments as a potential “killer use case” for digital ID wallets. The argument is primarily behavioral: payment transactions occur frequently, whereas ID transactions are less frequent. Integrating payment functionality could therefore normalize wallet usage through daily repetition, lowering behavioral barriers and accelerating adoption. Participants suggested that embedding payments may create habitual engagement, increasing exposure to ID functionalities that would otherwise remain infrequently used. In this view, payment functionality acts as an adoption accelerator rather than merely an additional feature.

However, regulatory assessments highlight structural tensions that complicate such integration. A report by the Dutch Payments Association (2025) notes that payments and digital ID operate under distinct regulatory frameworks within the EU, particularly under eIDAS 2.0 and PSD2. While the revised eIDAS regulation requires certain payment service providers to accept the EUDIW in processes requiring SUA, the report emphasizes significant legal and operational ambiguities. In particular, the EUDIW is interpreted as a potential two-factor authentication 2FA tool, yet SUA under PSD2 entails broader and more complex requirements. The report concludes that, at present, integrating the EUDIW into SUA processes appears operationally and legally challenging without further regulatory clarification.

These findings suggest that while payments may function behaviorally as a frequency anchor, their integration into digital ID wallets is institutionally constrained. The complexity of aligning ID regulation (eIDAS) with payment regulation (PSD2) introduces legal, liability, and operational challenges that may limit the strategic feasibility of wallet-payment convergence. Payments therefore represent both an adoption opportunity and a governance coordination challenge. Moreover, integrating payments into ID wallets could complicate data minimization principles or blur functional boundaries between identification and financial profiling.

Future research should examine whether integrating payments meaningfully increases ID wallet adoption, and under which regulatory or architectural conditions such convergence remains compatible with decentralized ID principles.

6.2.2 Should Identity Ecosystems Be Approached Like Payment Ecosystems?

A separate but related question concerns strategic transferability. Platform and payment literature heavily informs many adoption strategies identified in this thesis (including network activation, asymmetric pricing, and cross-side incentives). However, ID ecosystems may differ structurally from payment ecosystems in several important respects. Most notably, financial incentive mechanisms that are common in payment markets (such as cashback, reward schemes, or discounts) are largely absent in digital ID deployments. Interviewees confirmed that direct monetary incentives for end-users are rarely used in ID ecosystems. This raises a critical question:

Is the absence of financial incentives due to the early-stage and non-normalized status of ID wallets, or does it reflect a deeper structural difference between ID and payment markets?

Payments involve immediate financial exchange and clearly quantifiable consumer benefit (e.g., discounts, transaction speed). ID transactions, by contrast, are often compliance-driven, low-frequency, and infrastructural. The perceived value proposition may therefore be less suited to short-term promotional tactics. Furthermore, ID systems often involve public-sector actors and trust frameworks that constrain aggressive commercial growth strategies. In the regulated ID ecosystem, adoption strategies may be more tightly bound to governance design and institutional legitimacy than to market competition dynamics.

This suggests that while certain platform strategies are transferable, others may be context-dependent. Future research should systematically compare payment and identification ecosystems to identify which adoption mechanisms are structurally compatible and which are constrained by regulatory, behavioral or normative differences.

6.3 Applicability of the Framework to Government-Issued Wallets (EUDIW)

The multi-domain framework developed in this study is not limited to commercially driven wallet providers (private wallets). It is also applicable to government-issued or government-backed wallet ecosystems such as the EUDIW (public wallets). However, its applicability is not symmetrical. In public wallet settings, the five strategic domains remain relevant, but their relative weight shifts because adoption is shaped more strongly by institutional design, public policy objectives, and the role of the state as ecosystem orchestrator. In this sense, the framework remains applicable, but the strategic configuration is more strongly shaped by institutional structures, as public wallet providers operate within and partly define the governance environment, rather than only responding to it.

In particular, the **institutional structuring of adoption** domain becomes even more central in government-issued wallet contexts. In commercial wallet ecosystems, providers must navigate regulation, certification routes, and permissible ecosystem roles. In the public wallet context, by contrast, these structures are not just external conditions to which providers respond, they are partly built into the architecture of the ecosystem itself. Public authorities and EU-level governance arrangements define trust frameworks, liability structures, accepted credential models, and the conditions under which public and private actors may participate. As a result, institutional structuring is not only a strategic domain within the configuration but also the domain through which the overall shape of the ecosystem is largely determined.

At the same time, stronger institutional anchoring does not eliminate the relevance of **ecosystem orchestration & network activation**. Even when a wallet is publicly backed, adoption still depends on whether RPs, issuers, and intermediaries actually embed it into service journeys. Public issuance does not automatically generate integration, nor does regulatory legitimacy by itself guarantee cross-side participation. Wallet adoption still requires service-side activation, partner alignment, onboarding support, and sequencing decisions regarding which sectors and use cases are prioritized first. In that sense, even a government-issued wallet remains dependent on ecosystem orchestration to translate institutional availability into real usage.

The relevance of **user enablement & value proposition design** also persists in public wallet environments, although its role changes somewhat. A public wallet may rely less on competitive differentiation or brand-based positioning than a commercial provider, but users still need a reason to adopt and repeatedly use it. Ease of use, low-friction onboarding, understandable privacy features, recovery options, and meaningful service integration remain important. Public legitimacy may reduce certain barriers to initial trust, but it does not substitute for usability or perceived usefulness. Especially in voluntary settings such as the EUDIW, even state-backed wallets must still solve the problem of why users would actively choose to install and use the wallet in everyday contexts.

The domain of **incentive alignment and monetization architecture** is likewise still relevant, but its logic changes in a public wallet setting. In commercial ecosystems, this domain concerns revenue models, cross-subsidization, and the distribution of participation costs across market sides. In government-issued wallets, direct monetization may become less central, but the underlying coordination problem remains: implementation, operation, and integration still generate costs, and these costs must still be allocated across actors. The central question therefore shifts from who can be monetized to who bears the burden of adoption. For public wallets, incentive alignment becomes less a matter of pricing strategy and more a matter of governance, funding design, and the distribution of implementation responsibilities between public institutions and market actors.

Finally, **trust & legitimacy construction** remain crucial, but the sources of legitimacy differ from those in commercial contexts. Government-issued wallets may benefit from formal institutional authority, legal recognition, and public trust frameworks from the outset. However, this does not automatically resolve all trust-related barriers. Users may still worry about privacy, surveillance, or state overreach, while RPs may still require clarity on liability, compliance, and operational risk. Thus, even in public wallet ecosystems, legitimacy must still be actively constructed and maintained. The main difference is that trust is built less through competitive market signaling and more through public governance credibility, transparent safeguards, and institutional accountability.

This also highlights the role of the European Commission as an ecosystem actor. In the EUDIW context, the Commission is not only a regulator standing outside the market, but an actor that actively shapes the institutional conditions under which adoption becomes possible. Through legislative design, interoperability requirements, trust list structures, and implementation initiatives, the Commission co-configures the strategic environment for wallet adoption. This means that in public wallet ecosystems, adoption strategy is not designed solely by wallet providers themselves (the member states). It is partly distributed across policy actors, member states, and ecosystem intermediaries who together shape the feasible pathways of adoption. The Commission therefore occupies a dual role: it both defines the institutional architecture and influences the activation conditions under which the wallet can diffuse across the market.

Taken together, these observations suggest that the multi-domain framework remains applicable to government-issued wallets such as the EUDIW, but public issuance alters the balance between the domains. Institutional structuring becomes more dominant,

trust and legitimacy are more strongly tied to public authority, and incentive alignment shifts from monetization logic to governance and cost allocation. At the same time, public backing does not remove the need for orchestration, usability, or ecosystem participation. Government-issued wallets therefore do not invalidate the framework; rather, they reveal that the same strategic domains operate under a different configuration, one in which policy actors play a more direct role in shaping adoption outcomes.

While the framework thus appears applicable across both private and public wallet ecosystems, this discussion also indicates that its operation is context-dependent. In particular, the degree of regulatory enforcement, voluntariness, and public coordination may alter the relative importance of the domains. The following section therefore reflects on the boundary conditions under which the multi-domain framework holds.

6.4 Boundary Conditions of the Multi-Domain Framework

While the multi-domain framework provides a structured way to understand digital ID wallet adoption as a configurational process, the findings also indicate that its applicability is not unconditional. Rather than representing a universally stable model, the framework operates within a set of boundary conditions that shape when and how the strategic domains interact. These conditions determine the extent to which adoption remains a coordination problem between multiple actors, or shifts toward a more institutionally driven process.

A first key boundary condition concerns the degree of regulatory enforcement and coercion. The framework is grounded in the assumption that wallet adoption emerges through the coordinated activation of both users and RPs. However, in contexts where regulatory mandates are strong and strictly enforced, this coordination logic may be partially substituted by institutional force. As shown in the empirical findings, enforcement can compel RP participation even in the absence of strong voluntary demand, effectively replacing early-stage network activation mechanisms. In such cases, institutional structuring does not just condition strategy but becomes the dominant driver of adoption. This shifts the role of other domains. Ecosystem orchestration becomes less about voluntary partner activation and more about compliance implementation, while user adoption may follow from enforced exposure rather than intrinsic value creation. The framework therefore holds most strongly in settings where participation remains at least partly voluntary, and weakens when adoption is primarily mandate-driven.

A second boundary condition relates to the degree of voluntariness on the user side. The framework assumes that users must be actively convinced to adopt and use the wallet through perceived usefulness, ease of use, and trust. However, when wallet usage becomes mandatory, either directly through legal obligation or indirectly through lack of alternatives; user enablement strategies may lose explanatory power. In such scenarios, adoption may occur despite limited perceived value, and usage becomes a function of necessity rather than preference. This creates a fundamentally different adoption dynamic, in which behavioral determinants play a reduced role. At the same time, excessive coercion may introduce resistance, avoidance behavior, or legitimacy concerns, indicating that voluntariness is not only a condition for adoption mechanisms, but also for long-term acceptance.

A third boundary condition concerns the availability of meaningful use cases and intrinsic value creation. The framework presumes that adoption can be sustained through reinforcing feedback between user value and RP participation. However, as illustrated in the AV case, some use cases exhibit weak intrinsic demand and are primarily compliance-driven. In such contexts, user-side value creation is limited, and adoption depends heavily on regulatory enforcement and RP integration rather than on perceived usefulness. This suggests that the framework operates differently across use-case types. In high-value, high-frequency contexts, such as payments, user enablement and incentive alignment play a stronger role. In low-value, regulation-driven contexts, institutional structuring and RP onboarding dominate the adoption process. The framework therefore holds across use cases, but the relative importance of domains varies significantly.

A fourth boundary condition is the level of ecosystem maturity and market readiness. The framework assumes a setting in which ecosystem actors are capable of participating, integrating, and coordinating. However, in early-stage or fragmented environments, adoption may be constrained by missing infrastructure, lack of standards, or insufficient awareness among users and RPs. In such cases, even well-designed strategies may fail to produce adoption because the underlying ecosystem is not yet ready to support cross-side interaction. Conversely, in highly mature ecosystems with established trust frameworks and widespread digital infrastructure, some strategic challenges (such as initial trust building or onboarding friction) may be less pronounced. This indicates that the framework is most informative in transitional phases, where ecosystem formation and adoption dynamics unfold simultaneously.

Finally, the findings point to a broader boundary condition related to the hybrid governance nature of digital ID ecosystems. Unlike purely market-driven platforms, digital ID wallets operate at the intersection of public and private coordination. As a result, adoption strategies are not fully controlled by individual providers but are co-shaped by regulators, public institutions, and ecosystem intermediaries. This limits the extent to which strategic domains can be independently configured by wallet providers. In highly regulated environments such as the EUDIW, institutional actors may directly influence or constrain strategic choices, particularly in areas such as monetization, interoperability, and participation rules. The framework therefore assumes a degree of strategic agency that may be reduced in strongly governed ecosystems.

Taken together, these boundary conditions suggest that the multi-domain framework is best understood as a context-dependent analytical model rather than a universal adoption blueprint. It provides explanatory power in settings where adoption emerges through multi-actor coordination under partial voluntariness and evolving institutional structures. However, its dynamics shift when coercive regulation dominates, when user choice is limited, or when intrinsic value creation is weak. Under such conditions, adoption may become less a function of strategic configuration and more a result of institutional imposition.

These insights refine the contribution of the framework by clarifying not only how adoption strategies interact, but also under which conditions this interaction meaningfully explains adoption outcomes in digital ID ecosystems.

7 Implications and Conclusions

This section presents the conclusions and implications of the study. It begins with managerial implications for consulting practitioners and private wallet providers derived from the multi-domain framework (chapter 7.1). This is followed by a critical reflection on the limitations of the study (chapter 7.2). A future outlook then identifies points for potential future research that emerge from the findings (chapter 7.3). The section concludes with the overall conclusions of the study, addressing the central research question and sub-questions (chapter 7.4).

7.1 Managerial Implications

This study provides several practical implications for actors involved in the design, deployment, and governance of digital ID wallet ecosystems. Given the multi-sided and institutionally embedded nature of wallet adoption, the findings highlight that successful roll-out requires coordinated strategic action across multiple domains rather than isolated interventions.

Implications for Consulting and Strategy Practice

From a practitioner perspective, the framework offers a structured tool for navigating the complexity of digital ID ecosystems. In particular, it provides a shared conceptual reference grounded in empirical research, enabling more structured and evidence-based discussions with clients. In addition, the framework works as a diagnostic tool for identifying bottlenecks, allowing practitioners to assess whether adoption challenges stem from institutional constraints, lack of RP integration, weak user value, misaligned incentives, or insufficient trust. Furthermore, it provides a way to structure strategic conversations, helping align diverse stakeholders (e.g., regulators, wallet providers, RPs, intermediaries) around a common understanding of adoption dynamics. Lastly, it could be used as coordination tool in multi-stakeholder environments, enabling earlier alignment on roles, dependencies, and sequencing decisions. Overall, the framework reduces complexity by translating fragmented ecosystem challenges into a coherent strategic configuration.

Implications for Wallet Providers (Private Wallets)

For private wallet providers, the framework shows that no single strategy drives adoption. Wallet providers must configure multiple domains simultaneously (institutional positioning, RP activation, user enablement, incentive design, and trust construction). Weakness in one domain undermines all others. This highlights several strategic priorities. First, institutional positioning should precede market activation. Before investing in user acquisition or RP onboarding, providers must establish their regulatory standing (including certification, compliance with eIDAS/EUDIW requirements, and alignment with state governance structures). Without this foundation, other strategic efforts are unlikely to generate sustained participation. Second, RP onboarding should be treated as the primary adoption lever. Because users typically encounter the wallet through RP-embedded service flows rather than seeking it out independently, investment in RP integration support, liability clarity, and partnership activation will generate more adoption impact than consumer-facing marketing in early roll-out phases. Third, use cases should be selected strategically rather than purely on functional grounds. High-frequency, low-assurance use cases can serve as habit-forming entry points that build user familiarity and ecosystem density, while high-value, low-frequency use cases may serve as primary revenue sources. In voluntary contexts such as AV, where intrinsic user demand is weak, use case viability depends primarily on regulatory enforcement rather than user-driven adoption. Providers should evaluate use cases not only for their immediate utility but for their ability to create frequency and reduce switching costs over time. Fourth, the wallet should be designed as free-to-user from the outset. Users expect identity services to be free, and attempts to charge users directly are likely to suppress adoption. Monetization should instead be structured around RPs and high-assurance transactions, with cross-subsidization models supporting ecosystem growth in early phases. Fifth, trust construction should be treated as an institutional priority rather than a UX feature. For RPs, trust is a prerequisite for participation rather than a perception variable. Providers must therefore invest in certification signals, institutional partnerships, and governance alignment, not only in user-facing privacy communication. Finally, strategy configurations must be adapted to local market conditions. Cross-border regulatory fragmentation, cultural variation in institutional trust, and uneven enforcement intensity mean that adoption strategies that work in one market may not transfer directly to another. Providers should treat the framework as a diagnostic tool for identifying which domains require most attention in each specific deployment context.

7.2 Limitations and Reflexive Considerations

Sampling Scope This study relies on purposive expert sampling within a relatively small and highly interconnected professional community. Although this enabled access to strategically positioned actors with deep experience, it also introduces potential network bias. A substantial share of participants were recruited through professional and academic networks, which may partially reflect overlapping ecosystems of expertise. Although efforts were made to diversify roles and organizational types, the sample cannot be considered fully independent of professional network structures within the EUDI domain.

Snowball sampling was encouraged but resulted in limited expansion. Many suggested contacts were already included in the sample, while other recommended individuals did not respond or were outside the defined scope of the study. This limited snowball effect likely reflects both the small size of the expert population and the tight interconnections within the field. Additionally, parts of the data collection period coincided with holiday periods, which may have reduced response rates and limited availability for follow-up recruitment.

Absence of Big Tech Perspectives Efforts were made to include representatives from Big Tech firms active in digital ID and wallet ecosystems (e.g., Google, Apple, Amazon). Interviewees were asked whether introductions could be facilitated, and direct outreach was conducted via LinkedIn. However, no participation from these actors was secured within the timeframe of the study. The absence of Big Tech perspectives constitutes a limitation, particularly given their potential influence on wallet ecosystems, standardization processes, and adoption dynamics. Notably, several interviewees discussed the role of large platforms in shaping digital ID and AV landscapes; for example, through standardization involvement, mobile driver's license (mDL) and digital ID initiatives in the US (Apple Inc., 2025), AV integrations in app stores (Apple Inc., 2026), or AV-linked purchasing systems (Amazon Developer, 2026). However, these perspectives remain second-hand accounts rather than primary corporate viewpoints.

Future research could explicitly examine the strategic positioning of Big Tech providers in relation to regulated digital ID wallet ecosystems.

Form of Interview (Online vs. In-Person) Interviews were conducted both in person and online. While no systematic differences in depth or openness were observed, it is possible that interview format influenced interaction dynamics. In-person interviews may facilitate stronger rapport and informal exchange, whereas online interviews may create more structured and time-bound interactions. One online interview experienced minor technical difficulties (temporary audio disruptions), which slightly extended the duration of the session. However, the discussion was resumed without loss of substantive content, and the extended time allowed all core themes to be covered in full. Given the professional and strategic nature of the topics discussed, and the consistency of the semi-structured guide, the form of the interview is not considered to have materially affected thematic outcomes.

Interview Duration and Institutional Constraints One interview (conducted with a government representative involved in the Dutch national wallet initiative) lasted 31 minutes, compared to the typical 55-70 minute duration of the other interviews. The shorter duration reflects the institutional boundaries and policy-sensitive nature of the discussion. Certain strategic or operational details were classified or not publicly shareable. Within these constraints, all relevant governance-level adoption themes were covered. The limitation therefore concerns depth of disclosure rather than absence of perspective.

More broadly, several interviewees indicated that certain commercial strategies, partnership arrangements, or competitive positioning decisions could not be discussed in detail due to confidentiality constraints. In some cases, participants explicitly distinguished between publicly shareable insights and what they described as more sensitive “core strategic” elements. As a result, discussions often shifted toward personal reflections, industry-level observations, or general strategic reasoning rather than organization-specific operational details. While this dynamic is common in elite interviewing contexts, it may have limited direct visibility into actual strategic decision-making processes (Richards, 1996).

Self-Reflection and Elite Interview Bias As with many expert-based qualitative studies, findings rely on retrospective self-reporting. Interviewees may frame past strategies in a favorable light, rationalize unsuccessful initiatives, or selectively emphasize certain challenges (Richards, 1996). While efforts were made to probe inconsistencies and encourage discussion of failures or trade-offs, the data reflects participants' interpretations of strategic processes rather than independently verified operational records. At the same time, most participants held senior or executive roles with extensive professional experience, which enhances the strategic relevance of their reflections. The study therefore prioritizes depth of insight over objective behavioral measurement.

Temporal Sensitivity of the Topic Digital ID and AV are rapidly evolving regulatory and technical domains. Legislative frameworks (e.g., eIDAS 2.0, DSA implementation guidelines), certification standards, and interoperability requirements are still under development. As a result, some strategic assessments or ecosystem expectations expressed by interviewees may become outdated as regulatory enforcement intensifies or market structures stabilize. The findings should therefore be interpreted as reflecting a particular moment in the evolution of regulated digital ID wallet ecosystems.

Privacy-Conscious Sample Characteristics Several participants expressed strong views on data protection, platform power, and Big Tech influence. Some reported limited use of social media or commercial (payment) wallet services themselves. While this may reflect broader trends within digital ID communities, it is possible that the sample over-represents privacy-conscious or sovereignty-oriented perspectives. This could shape how risks, governance, and ecosystem dynamics are framed in the findings.

7.3 Future Outlook

This study provides a literature-informed and empirically enriched framework for analyzing adoption strategies in regulated digital ID wallet ecosystems. However, given the early-stage and rapidly evolving nature of the EUDI ecosystem, several important points for future research emerge.

Sustainable Funding Models and User Willingness to Pay One central open question concerns the long-term economic sustainability of digital ID wallets. While most interviewees rejected direct user charging under current market conditions, some suggested that a user-pays model could, in principle, better align providers with user privacy interests and reduce dependence on RP-side cross-subsidization. Future research could examine:

- user willingness-to-pay across different ID use cases (e.g., high-assurance financial transactions versus low-assurance access control),
- comparative sustainability of RP-funded, government-funded, and user-funded models, and

- the impact of funding structure on governance design, incentive alignment, and data minimization outcomes.

Such research would clarify whether the prevailing “free-to-user” model reflects structural constraints of ID ecosystems or a transitional market convention.

Identity-Payment Convergence and Cross-Domain Integration Payments were frequently described as a potential “frequency anchor” capable of accelerating wallet adoption. However, ID and payment systems operate under distinct regulatory and liability regimes, and recent regulatory assessments highlight significant integration complexities. Future research could explore whether integrating payment functionality meaningfully accelerates ID wallet adoption in practice and whether ID-payment convergence strengthens or undermines decentralization, privacy-by-design, and functional separation principles. Also, comparative analysis of identity-centric versus payment-centric wallet models may reveal whether cross-domain strategic transferability is feasible or structurally constrained.

The Strategic Role of Large Platform Providers Although major technology firms did not participate directly in this study, their presence appeared a lot in practitioner narratives. Firms such as Apple and Google are increasingly active in digital ID, mobile driver’s licences, and wallet standardization initiatives. Future research could investigate how global platform providers position themselves relative to the sovereign EUDI initiative and whether their participation accelerates diffusion, introduces competitive tensions, or reshapes governance dynamics. Given ongoing debates around digital sovereignty of the EU, platform power, and infrastructure control, this dimension requires systematic empirical analysis.

Longitudinal Analysis in an Evolving Regulatory Environment This study captures adoption strategies during an early implementation phase of eIDAS 2.0 and the DSA. As enforcement intensifies and standards mature, adoption dynamics may shift significantly. Longitudinal research could examine how strategy configurations evolve as mandates move from voluntary to semi-mandatory environments, whether early-stage ecosystem activation mechanisms remain effective under institutional stabilization and how market structure and competitive positioning consolidate over time. Such research would deepen understanding of how regulated digital infrastructures transition from innovation phase to operational normalization.

Beyond Expert Perspectives: Behavioral Validation This study relies primarily on expert reflections regarding adoption strategies. While strategically insightful, these perspectives would benefit from behavioral validation. For this, future studies could incorporate: large-scale user surveys, experimental testing of trust and usability interventions, RP-side cost–benefit modeling and pricing sensitivity experiments in ID contexts. This would allow triangulation between strategic intent and actual participation behavior.

Secondary Analytical Potential of the Dataset Beyond the scope of the present research questions, the dataset generated in this study offers additional analytical potential. The interviews contain rich material on: emerging business model experimentation, public-private governance tensions, market positioning strategies under regulatory uncertainty and the evolving infrastructure framing of digital ID. Future research could draw on this material to examine digital ID wallets from a business model innovation perspective or through institutional theory lenses. In particular, the interaction between regulatory architecture and monetization logic presents a promising base for further conceptual development.

7.4 Conclusions

This study set out to answer the central research question:

What adoption strategies could wallet providers consider when rolling out digital identity wallets?

The findings demonstrate that digital ID wallet adoption is not the result of a single optimal tactic, but rather of a coordinated configuration of interdependent strategic domains operating within institutional constraints. Adoption emerges when providers align regulatory positioning, ecosystem activation, user-side value design, economic incentives, and legitimacy construction in a mutually reinforcing manner.

RQ1: *What adoption strategies emerge from the literature and past digital identity and wallet initiatives?*

The literature review identified seven literature-derived strategy families: governance & ecosystem orchestration, trust & legitimacy, user-side value, RP-side value, network activation, pricing & incentive mechanisms, and staging & sequencing. These strategies address recurring adoption challenges in digital ID and platform ecosystems, including chicken-and-egg coordination failure, trust deficits, perceived cost barriers, and ecosystem fragmentation.

Synthesizing these strands led to a layered conceptual framework in which governance conditions shape strategy design, strategies influence behavioral determinants (trust, usefulness, risk, cost), and adoption decisions generate cross-side network effects. The literature therefore conceptualizes adoption as a systemic, multi-layered process mediated by behavioral and institutional factors rather than purely technical features.

RQ2: *How do expert practitioners evaluate, validate, and enrich this framework?*

Empirical findings from 18 interviews broadly validated the literature-derived strategy families but significantly enriched them. First, adoption did not unfold as a linear layered mechanism. Instead, practitioners described adoption as a configurational coordination process, in which five interdependent strategic domains must be aligned in parallel: Institutional Structuring of Adoption, Ecosystem Orchestration & Network Activation, User Enablement & Value Proposition Design, Incentive Alignment & Monetization Architecture and Trust & Legitimacy Construction. Second, the empirical analysis revealed that regulation can function not merely as a background condition, but as an active activation mechanism, substituting for missing early-stage network effects in the highly regulated ID market. Third, trust emerged as a dual-level mechanism: privacy reassurance and non-traceability are central for users, while certification, compliance assurance, and institutional legitimacy are decisive for RPs. This highlights the asymmetric and multi-level nature of trust in digital ID ecosystems. Fourth, incentive alignment was shown to operate as a cross-domain coordination mechanism. Rather than functioning solely as pricing tactics, cost allocation and monetization architecture shape participation dynamics across both sides of the market.

Taken together, the empirical findings shift the understanding of wallet adoption from a layered causal sequence to a reinforcing configuration of strategic mechanisms operating under structural constraints.

RQ3: How applicable are the validated strategies to a voluntary, platform-dependent use case, specifically age verification (AV) as a precursor to the EUDIW, and what AV-specific measures should wallet providers consider?

The application of the framework to the AV use case demonstrated that the configurational logic remains valid, but domain weightings shift substantially. In AV, institutional structuring becomes the dominant activation lever, as regulatory enforcement substitutes for weak voluntary demand. Ecosystem orchestration is strongly RP-gated, with adoption primarily triggered through service integration rather than user pull. User enablement shifts from intrinsic value creation to normalization and stigma management. Incentive alignment is constrained by limited willingness to pay and uncertain commercial viability. Trust construction operates at two levels: visible privacy reassurance for users and formal institutional legitimacy for RPs. AV therefore does not function as an automatic precursor to broader wallet adoption. Instead, it represents a regulation-triggered, low-assurance, platform-dependent use case whose strategic value depends on enforcement intensity, governance credibility, stigma mitigation, and integration within a broader digital identity ecosystem. For wallet providers, AV should be approached either as: a compliance-driven ecosystem entry point, or a habit-forming feature embedded within a broader multi-purpose wallet, rather than as a standalone commercial product.

Overall, this study demonstrates that digital ID wallet adoption is fundamentally a multi-sided coordination challenge embedded in institutional governance structures. Sustainable wallet roll-out depends not on isolated strategic interventions, but on the coherent alignment of regulatory positioning, ecosystem activation, user value design, incentive structures, and legitimacy construction within a constrained and fragmented environment.

By re-conceptualizing wallet adoption as a configurational and institutionally embedded process, this thesis contributes a grounded framework that can guide both practitioners and policymakers navigating the complex roll-out of digital ID infrastructures in Europe and beyond.

The digital ID ecosystem remains in an early and formative phase, shaped by ongoing regulatory developments and experimentation across public and private actors. As standards mature and enforcement intensifies, today's strategic differentiators may diminish, potentially transforming wallets into commoditized infrastructural components. In such an evolving environment, sustained adoption will depend not on isolated innovations, but on the coherent alignment of institutional, economic, and ecosystem mechanisms.

Acknowledgments

I would like to express my sincere gratitude to Prof. Mark de Reuver for his supervision, insightful feedback, and the many constructive discussions throughout this project. His expertise and guidance were invaluable in shaping the scientific direction of this thesis. I am especially grateful for his support in connecting me with INNOPAY, which ultimately became the setting of my graduation internship and an integral part of this research.

I am also grateful to Dr. Zenlin Roosenboom-Kwee for serving on my graduation committee as 2nd supervisor and for the constructive feedback provided during the formal evaluation meetings.

I would also like to thank Henk Marsman for his valuable industry insights, thoughtful literature suggestions, and his support in the recruitment of interviewees. His willingness to share knowledge and to help reach out to participants significantly strengthened this research.

My sincere appreciation goes to my supervisors at INNOPAY, Vincent Jansen and Leon Kluiters, for their continuous support and engagement. Our weekly meetings and in-depth discussions greatly enriched both the academic and practical dimensions of this thesis. I am particularly grateful for their efforts in reaching out to their professional networks and sending introductory invitations to potential participants. Without their support, it would not have been possible to conduct such a substantial number of interviews. Their deep industry expertise provided invaluable context and perspective throughout the project.

I would also like to thank my colleagues at INNOPAY for making this internship both professionally rewarding and personally enjoyable. A special thanks to Beau, Jeroen and Thomas for their help in connecting with potential participants and supporting the outreach process.

Furthermore, I am sincerely grateful to all anonymous interviewees who generously contributed their time, knowledge, and perspectives to this research. Their openness and willingness to participate formed the foundation of this study.

I would also like to thank my friends for their encouragement and support, as well as for taking the time to read parts of this thesis, helping me improve clarity and catch overlooked errors.

Finally, I thank my family for their continuous support, motivation, and patience throughout this entire process. Their encouragement has meant more to me than words can express.

Use of AI Tools

Artificial intelligence (AI) tools were used in a limited, supportive capacity during the development of this thesis. Specifically, OpenAI's ChatGPT was employed for the following purposes:

- Writing support: Rephrasing and editing selected text sections to improve clarity, grammar coherence, and academic tone, without altering the scientific meaning.
- Structural support: Assisting in brainstorming, organizing ideas, and improving the logical flow of sections when refining arguments.
- LaTeX support: Helping resolve formatting issues and structuring equations, tables, and references in LaTeX.
- Literature processing support: Summarizing long academic articles to facilitate an initial overview of key arguments, while all cited sources were read in full and critically assessed by the author.
- During the qualitative analysis phase, AI was occasionally consulted to help refine the wording of emerging themes and to explore alternative ways of structuring preliminary categorizations. However, all interviews were coded manually by the author, and the development of themes, interpretation of findings, and theoretical integration were conducted independently. AI tools were not used to automatically analyse interview transcripts or to generate findings.

All literature review and sourcing of references were conducted independently by the author, and all cited material was read and critically assessed by the author. AI tools were **not** used to generate scientific content, conduct data analysis, or interpret results. Their use was limited to technical and editorial support.

All AI-assisted outputs were carefully reviewed and revised by the author. The author assumes full responsibility for the content, originality, and scientific integrity of this thesis.

References

- Age Check Certification Scheme. (2025, August). *Age assurance technology trial: Part a – main report* (tech. rep.) (Funded by the Commonwealth of Australia. Prepared by the Age Check Certification Scheme.). Commonwealth of Australia. <https://ageassurance.com.au/an-impartial-approach/>
- Age Check Certification Scheme Limited. (2025). *ACCS 1:2025 Certification Scheme for Age Assurance Systems and Components* (Certification Standard) (Aligned with ISO/IEC 27566-1:2025 and IEEE 2089.1:2024). Age Check Certification Scheme Limited.
- Amazon Developer. (2026, January). *User age verification*. Retrieved February 26, 2026, from <https://developer.amazon.com/docs/app-submission/user-age-verification.html>
- Apple Inc. (2025). Id in wallet [Retrieved 13 Oct 2025]. <https://learn.wallet.apple/id>
- Apple Inc. (2026, February). *Age requirements for apps distributed in brazil, australia, singapore, utah, and louisiana* [Apple Developer News. Accessed 26 February 2026]. <https://developer.apple.com/news/?id=f5zj08ey>
- Aziz, E. (2025). *Digital wallet ecosystem: Case study to explore creation, governance and value dynamics in platform ecosystems* [Tesi magistrale in Management Engineering (Ingegneria Gestionale)]. Politecnico di Milano [Executive summary of the thesis; Academic year 2023–2024]. <https://hdl.handle.net/10589/235013>
- Caillaud, B., & Jullien, B. (2003). Chicken egg: Competition among intermediation service providers. *The RAND Journal of Economics*, 34(2), 309–328. Retrieved October 13, 2025, from <http://www.jstor.org/stable/1593720>
- Cespiva, R. B. (2018). *Factors influencing the decision to adopt a digital identity: A correlational study* [D.I.T. Dissertation]. Capella University, School of Business and Technology [ProQuest Dissertation No. 10937601]. <https://www.proquest.com/docview/2124445405>
- Coulmas, F. (2019, February). *Identity: A very short introduction*. Oxford University Press. <https://doi.org/10.1093/actrade/9780198828549.001.0001>
- Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets*, 34(1), 50. <https://doi.org/10.1007/s12525-024-00731-1>
- Delft University of Technology. (2026). *Human research ethics*. Retrieved February 24, 2026, from <https://www.tudelft.nl/over-tu-delft/strategie/integriteitsbeleid/human-research-ethics>
- de Reuver, M., Nederstigt, B., & Janssen, M. F. W. H. A. (2018). Launch strategies for multi-sided data analytics platforms [Conference paper]. *Conference Paper*. <https://resolver.tudelft.nl/uuid:e7a2d28b-9b73-4c9a-9443-a5c64a28d29a>
- DigiD. (2025). What is DigiD? [Retrieved 13 Oct 2025]. <https://www.digid.nl/en/what-is-digid/>
- Dutch Payments Association. (2025, May). *The eu digital identity wallet in payments: Interpretation of legislators' intention and feasibility assessment* (Industry Report) (Retrieved 07 Oct 2025). <https://www.betalvereniging.nl/wp-content/uploads/EUDIW-in-payments-Interpretation-of-legislators-intention-and-feasibility-assessment.pdf>
- European Commission. (n.d.). *The EU approach to age verification* [An Official Website of the European Union; Retrieved 08 Oct 2025]. <https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification>
- European Commission. (2025a). *European age verification solution* [Retrieved 07 Oct 2025]. <https://ageverification.dev/>
- European Commission. (2025b). *The many use cases of the EU digital identity wallets* [Retrieved 13 Oct 2025]. <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/716146139/The+many+use+cases+of+the+EU+Digital+Identity+Wallet>
- European Commission. (2025c). *What are EU digital identity wallets* [Retrieved 08 Oct 2025]. <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/791609471/What+is+the+Wallet>
- European Commission. (2025d). *What are the large scale pilots* [Retrieved 08 Oct 2025]. <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487808/What+are+the+Large+Scale+Pilot+Projects>
- Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065 (2025, October 10). <http://data.europa.eu/eli/C/2025/5519/oj>
- European Union. (2024a). Regulation (EU) 2024/1183 of the european parliament and of the council [EUR-Lex; An Official Website of the European Union; Retrieved 08 Oct 2025]. <https://eur-lex.europa.eu/eli/reg/2024/1183>
- European Union. (2024b). *What is age assurance?* [Better Internet for Kids (BIK) Portal. Accessed 26 February 2026]. <https://better-internet-for-kids.europa.eu/en/age-assurance-guide/explainers/what-age-assurance>
- Evans, D., & Schmalensee, R. (2010). Failure to launch: Critical mass in platform businesses. *Review of Network Economics*, 9, 1–1. <https://doi.org/10.2139/ssrn.1353502>
- Evans, D. S., & Schmalensee, R. (2016). *Matchmakers: The new economics of multisided platforms*. Harvard Business Review Press.
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the gioia methodology. *Organizational Research Methods*, 16(1), 15–31. <https://doi.org/10.1177/1094428112452151>

- Google. (2025). Google wallet [Retrieved 13 Oct 2025]. <https://wallet.google/digitalid/>
- Hilowle, M., Yeoh, W., Grobler, M., Pye, G., & Jiang, F. (2023). Users' adoption of national digital identity systems: Human-centric cybersecurity review. *Journal of Computer Information Systems*, 63(5), 1264–1279. <https://doi.org/10.1080/08874417.2022.2140089>
- Hofmann, S., Räckers, M., & Becker, J. (2012). Identifying factors of e-government acceptance - a literature review. *International Conference on Information Systems, ICIS 2012*, 4, 3022–3040.
- Hoskisson, R. E., & Hoskisson, M. W. (2025). Implementation of platform strategies: From initiation to critical mass and expansion to complementary networks [The Challenges of Strategy Implementation]. *Organizational Dynamics*, 54(4, Part 1), 101156. <https://doi.org/https://doi.org/10.1016/j.orgdyn.2025.101156>
- Husainah, N., Paulina, J., Misrofingah, Pradipta, I., Maulana, A., & Fahlevi, M. (2023). Determining factors of digital wallet actual usage: A new model to identify changes in consumer behavior. *International Journal of Data and Network Science*, 7. <https://doi.org/10.5267/j.ijdns.2022.12.017>
- iDIN. (2025). About iDIN [Retrieved 13 Oct 2025]. <https://www.idin.nl/en/about-idin/>
- Jackwerth-Rice, T., Baumann, W., Blind, K., Metzger, F., Martin, N., & Pullmann, L. (2023, December). *Identity management in public services: Report on the social perception and recommendations (d4.2, version 2.0)* (Deliverable Report No. D4.2). IMPULSE Project (Horizon 2020). <https://www.impulse-h2020.eu/public-deliverables/>
- Jacob, D. W., Fudzee, M. F. M., Salamat, M. A., & Herawan, T. (2019). A review of the generic end-user adoption of e-government services. *International Review of Administrative Sciences*, 85(4), 799–818. <https://doi.org/10.1177/0020852319861895>
- Jurison, J. (2000). Perceived value and technology adoption across four end user groups. *JOEUC*, 12, 21–28. <https://doi.org/10.4018/joeuc.2000100103>
- Kao, G., Hong, J., Perusse, M., & Sheng, W. (2020). The chicken or the egg. In *Turning silicon into gold: The strategies, failures, and evolution of the tech industry* (pp. 31–36). Apress. https://doi.org/10.1007/978-1-4842-5629-9_5
- Karhu, K., & Ritala, P. (2021). Slicing the cake without baking it: Opportunistic platform entry strategies in digital markets. *Long Range Planning*, 54(5), 101988. <https://doi.org/https://doi.org/10.1016/j.lrp.2020.101988>
- Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. *The American Economic Review*, 75(3), 424. Retrieved October 13, 2025, from <http://www.jstor.org/stable/1814809>
- Khatchatourov, A., Laurent, M., & Claire, L.-B. (2015). Privacy in digital identity systems: Models, assessment and user adoption. https://doi.org/10.1007/978-3-319-22479-4_21
- Kraiwanit, T., Limna, P., Wattanasin, P., Asanprakit, S., & Thetlek, R. (2023). Adoption of worldcoin digital wallet in thailand. *Research in Globalization*, 7, 100179. <https://doi.org/https://doi.org/10.1016/j.resglo.2023.100179>
- Krotoski, A., & Hammersley, B. (2015). Identity and agency. In *The international encyclopedia of digital communication and society* (pp. 1–9). John Wiley & Sons, Ltd. <https://doi.org/10.1002/9781118767771.wbiedcs094>
- Kubicek, H., & Noack, T. (2010). Different countries-different paths. extended comparison of the introduction of eids in eight european countries. *Identity in the Information Society*, 3. <https://doi.org/10.1007/s12394-010-0063-x>
- Kudra, A., Rieger, A., Sedlmeir, J., Roth, T., Fridgen, G., & Young, A. (2025). Digital identity wallets: A guide to the eu's new identity model. *Information Systems Journal*, 1–10. <https://doi.org/10.1111/isj.70009>
- Liezenberg, C., Lycklama, D., & Nijland, S. (2019). *Everything transaction* (1st English edition) [Self-published English edition, NUR 801]. INNOPAY International. <https://www.everythingtransaction.com/>
- McLaughlin, M., Malone, P., & Jennings, B. (2009). A model for identity in digital ecosystems. *2009 3rd IEEE International Conference on Digital Ecosystems and Technologies, DEST '09*, 295–300. <https://doi.org/10.1109/DEST.2009.5276727>
- Mohammed, I. A. (2021). Factors affecting user adoption of identity management systems: An empirical study. *International Journal of Innovations in Engineering Research and Technology*, 8(1), 104–110. <https://repo.ijert.org/index.php/ijert/article/view/2784>
- Murtezaj, D. (2023, November). *Unlocking digital trust: A study of user trust and usability in a digital identity wallet concept* [Master's thesis]. Freie Universität Berlin, Department of Computer Science [Submitted on 11 November 2023].
- Nguyen, H. (2017). *Solving chicken and egg dilemma in online platform startup: Value proposition in focus* [Master's thesis, Aalto University, School of Business] [Master's thesis, Management and International Business (MIB); Supervisor: Alexei Koveshnikov]. <https://urn.fi/URN:NBN:fi:aalto-201711137515>
- OECD. (2019). *Digital government in chile – digital identity*. <https://doi.org/10.1787/9ecba35e-en>
- Online Etymology Dictionary. (n.d.). *Identity* [Retrieved 07 Oct 2025]. <https://www.etymonline.com/word/identity>
- Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). *Platform revolution: How networked markets are transforming the economy and how to make them work for you* (First edition). W.W. Norton & Company.
- Podgorelec, B., Alber, L., & Zefferer, T. (2022). What is a (digital) identity wallet? a systematic literature review. <https://doi.org/10.1109/COMPSAC54236.2022.00131>

- Poller, A., Waldmann, U., Vowe, S., & Turpe, S. (2012). Electronic Identity Cards for User Authentication-Promise and Practice. *IEEE Security & Privacy*, 10(1), 46–54. <https://doi.org/10.1109/MSP.2011.148>
- Raman, M., & Edward, M. (2018). Consumer adoption towards digital payment wallets.
- Richards, D. (1996). Elite interviewing: Approaches and pitfalls. *Politics*, 16(3), 199–204. <https://doi.org/10.1111/j.1467-9256.1996.tb00039.x>
- Rowland, J., & Esteve, J. (2025). “what is your digital identity?” unpacking users’ understandings of an evolving concept in datafied societies. *Media, Culture & Society*, 47(2), 336–353. <https://doi.org/10.1177/01634437241282240>
- Rysman, M. (2009). The economics of two-sided markets. *The Journal of Economic Perspectives*, 23(3), 125–143. Retrieved October 13, 2025, from <http://www.jstor.org/stable/27740544>
- Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity [Blockchain Innovations: Business Opportunities and Management Challenges]. *Information Management*, 59(7), 103553. <https://doi.org/https://doi.org/10.1016/j.im.2021.103553>
- Sellung, R., & Kubach, M. (2023). Research on user experience for digital identity wallets: State-of-the-art and recommendations. <https://doi.org/10.18420/OID2023.03>
- Signicat. (2025). About Signicat [Retrieved 13 Oct 2025]. <https://www.signicat.com/about>
- Singh, S. (2013). *Business model analysis of mobitto – how to solve the chicken and egg problem of a multi-sided platform?* [Master’s thesis, NOVA School of Business and Economics] [Master’s thesis, Field Lab Entrepreneurial Innovative Ventures; Supervisor: Filipe Castro Soeiro].
- Stegfeller, A. (2025). *The coordination problem in two-sided platforms: Strategies for overcoming customer and provider acquisition* [Master’s thesis, Johannes Kepler University Linz] [Master’s thesis]. <https://urn:nbn:at:at-ubl:1-90239>
- Stummer, C., Kundisch, D., & Decker, R. (2018). Platform launch strategies. *Business & Information Systems Engineering*, 60(2), 167–173. <https://doi.org/10.1007/s12599-018-0520-x>
- Tammpuu, P., & Masso, A. (2019). Transnational digital identity as an instrument for global digital citizenship: The case of estonia’s e-residency. *Information Systems Frontiers*, 21. <https://doi.org/10.1007/s10796-019-09908-y>
- Tang, S., Wu, Z., Zhang, X., Wang, G., Ma, X., Zheng, H., & Zhao, B. (2019). Towards understanding the adoption and social experience of digital wallet systems. *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS)*, 10. <https://doi.org/10.24251/HICSS.2019.612>
- Tanriverdi, A. (2025, September). *Teel üleeuroopalise digirahakoti kasutuselevõtu poole: Tähelepanekud eesti ja belgia EUDI rahakoti rakendamisest. the road to EU-wide digital identity wallet adoption: Insights from estonia and belgium’s EUDI wallet implementation* [Master’s thesis]. Tallinna Tehnikaülikool (Tallinn University of Technology), Ma-jandusteaduskond / School of Business and Governance [Submitted on 8 September 2025].
- Teng, S., & Khong, K. W. (2021). Examining actual consumer usage of e-wallet: A case study of big data analytics. *Computers in Human Behavior*, 121, 106778. <https://doi.org/https://doi.org/10.1016/j.chb.2021.106778>
- UK Government. (2025, April). *Online safety act: Explainer*. Retrieved February 24, 2026, from <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#what-does-the-online-safety-act-do>
- Veseli, F., Olvera, J. S., Pulls, T., & Rannenberg, K. (2019). Engineering privacy by design: Lessons from the design and implementation of an identity wallet platform. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 1475–1483. <https://doi.org/10.1145/3297280.3297429>
- Windwehr, S., & Hancock, A. (2025, April). *Age verification in the european union: The commission’s age verification app* [Retrieved 07 Oct 2025]. <https://www.eff.org/deeplinks/2025/04/age-verification-european-union-mini-id-wallet>
- World Bank. (2022). *National digital identity and government data sharing in singapore: A case study of singpass and apex* (tech. rep.) (License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)). World Bank. Washington, DC.

8 Appendix

8.1 Adoption Strategies from Literature

Table 3: List of Literature-Derived Adoption Strategies.

#	Strategy	Definition	Target	Ref
1	Coring	Defining a core value proposition that addresses a systemic coordination or identity problem before scaling the platform.	System	(de Reuver et al., 2018)
2	Pricing for market entry	Structuring initial pricing to reduce participation barriers and stimulate early adoption on at least one side of the market.	User/RP	(D. S. Evans & Schmalensee, 2016)
3	Onboarding design	Designing friction-reducing onboarding processes to accelerate integration of users and partners.	User/RP	(de Reuver et al., 2018)
4	Platform openness	Allowing external actors to build on or integrate with the platform to foster ecosystem expansion.	RP/System	(de Reuver et al., 2018)
5	Platform leadership	Communicating long-term strategic commitment to reduce uncertainty and attract ecosystem participants.	System	(de Reuver et al., 2018)
6	Piggybacking	Leveraging existing infrastructure, networks, or installed bases to accelerate adoption and reduce coordination costs.	System	(Parker et al., 2016)
7	Seeding	Actively stimulating early participation through incentives, partnerships, or internal use cases to create initial liquidity.	User/RP	(Parker et al., 2016; Singh, 2013)
8	Micro-market focus	Targeting a narrowly defined segment to achieve critical mass before broader expansion.	System	(Parker et al., 2016)
9	Marquee users	Recruiting high-profile participants to signal credibility and attract additional adoption.	RP	(Nguyen, 2017; Parker et al., 2016)
10	Single-player mode	Offering standalone value to one side of the market before cross-side network effects fully develop.	User	(Kao et al., 2020)
11	Subsidizing one side (Penetration Pricing)	Temporarily lowering costs for one participant group to stimulate cross-side growth dynamics.	User/RP	(D. S. Evans & Schmalensee, 2016; Stummer et al., 2018)
12	Freemium model	Providing a free basic service tier while monetizing advanced features to balance growth and revenue.	User	(Nguyen, 2017)
13	Asymmetric pricing	Charging participant groups differently to optimise cross-side adoption incentives.	System	(D. S. Evans & Schmalensee, 2016)
14	Platform envelopment (Remora)	Entering adjacent markets by bundling complementary services to leverage an existing user base.	System	(Nguyen, 2017; Stummer et al., 2018)
15	Exclusivity agreements/Strategic Alliance	Securing exclusive partnerships to limit competition and strengthen ecosystem control.	RP	(Nguyen, 2017; Stummer et al., 2018)
16	Side-switching	Designing participation models that allow actors to engage across multiple sides of the platform.	System	(Stummer et al., 2018)
17	Platform staging	Expanding gradually across user groups or sectors to manage coordination complexity.	System	(Stummer et al., 2018)
18	Phased roll-out	Introducing functionality incrementally to reduce risk and enable iterative refinement.	System	(Hoskisson & Hoskisson, 2025)
19	Use-case prioritization	Identifying high-value processes where identity solutions deliver tangible early benefits.	User/RP	Case studies (e.g. World Bank (2022), OECD (2019))

#	Strategy	Paraphrased Definition	Target	Ref
20	Follow-the-rabbit	Embedding identity solutions into existing behavioural routines to reduce switching resistance.	User	(Parker et al., 2016)
21	Big-bang	Launching broadly with multiple partners to rapidly generate ecosystem scale.	System	(Parker et al., 2016)
22	Producer-evangelism	Actively promoting participation among service providers to accelerate integration.	RP	(Parker et al., 2016)
23	Platform exploitation	Leveraging incumbent ecosystem resources to accelerate competitive positioning.	System	(Karhu & Ritala, 2021)
24	Platform injection	Embedding the platform within an existing ecosystem to benefit from established user bases.	System	(Karhu & Ritala, 2021)
25	Platform pacing	Strategically timing feature releases and boundary resource development to manage growth.	System	(Karhu & Ritala, 2021)
26	Aggressive marketing	Investing heavily in awareness and acquisition efforts to accelerate critical mass formation.	User	(Nguyen, 2017)
27	Bundling and tying	Combining identity functionality with complementary services to enhance perceived value and lock-in.	User/RP	(Nguyen, 2017)
28	UX/User Communication strategies	Optimizing user experience and transparency of how their data is handled in the communication.	User	(Sellung & Kubach, 2023)

8.2 Interviewee List

Table 4: Interview Participant Anonymization List.

Anon ID	High-Level Group	Subgroup (Actor Type)	Sector	Experience Band in Digital ID	Geography (Broad)	Role
WP-7K2M	Wallet Provider	Wallet provider	Private	10-15 years	NL	Senior technical executive
WP-Q8R4	Wallet Provider	Wallet Provider	Private	5-10 years	NL/UK	Senior management
WP-3N9C	Wallet Provider	Wallet Provider	Private	0-5 years	BE/EU	Senior management
WP-L5T6	Wallet Provider	Wallet Provider	Private	5-10 years	NL	Architect
DIP-9R4K	Digital Identity Provider	Identity Platform / Initiative	Private	10-15 years	NL	Founding team member / Senior executive
DIP-Q7M2	Digital Identity Provider	Digital Identity Product	Private	10-15 years	NL	Management
DIP-5T8C	Digital Identity Provider	Identity Platform / Initiative	Public-Private	20+	UK/Global	Consultant (strategy/implementation of digital ID)
GOV-X9M4	Government / Policy	Government / Policy Maker	Public	0-5 years	NL	Management
DIB-X4P7	Digital Identity Broker	Identity Broker / Intermediary	Private	N/A	NL/ Global	Management
DIB-2K9R	Digital Identity Broker	Identity Broker / Intermediary	Private	15-20 years	NL/ Global	Senior management
DIB-M8Q3	Digital Identity Broker	Digital Identity Solutions Provider / White-label wallet infrastructure provider	Private	5-10 years	GE/EU	Senior management
DIB-5C7T	Digital Identity Broker	White-label digital identity infrastructure provider	Private	10-15 years	Australia/Asia (e.g. Japan) / Pacific / EU	Senior executive

Anon ID	High-Level Group	Subgroup / Actor Type	Sector	Experience Band in Digital ID	Geography (Broad)	Role
DIB-6O7F	Digital Identity Broker	Identity Broker / Intermediary	Private	0-5 years	EU/UK	Senior executive
AV-6T3R	Age Verification	AV solution provider (& Digital ID solution) / Wallet	Private	N/A	UK	Senior management
AV-Q2M9	Age Verification	Intermediary / Orchestrator	Private	20+ years	UK/ Global	Senior Management
AV-7C5K	Age Verification	Standards certification body	NGO	20+ years	UK/Global	Senior role
AV-N8P4	Age Verification	AV Consortium	Public	0-5 years	EU	Management
AV-S1U6	Age Verification	AV Consortium	Public	N/A	EU/Global	Management

8.3 Interview Guides

This appendix presents the semi-structured interview guides used for interviews with digital identity and AV experts. Both guides were designed as an internal researcher tool to elicit strategic insights into adoption challenges and solutions across digital identity ecosystems. Interviews were conducted flexibly, with questions prioritized and adapted based on participants' expertise and the direction of the conversation. The interview guide was not shared with participants in advance.

8.3.1 Interview Guide – Digital Identity Experts

Semi-Structured Interview Guide – Digital Identity Experts

0. Opening & Warm-Up

- **Interviewer:** Hi, thanks so much for taking the time to speak with me today. Before we start, how are you doing?
- **Interviewer:** Great — thanks again for participating. I really appreciate your willingness to share your experience.

1. Informed Consent Check

- **Interviewer:** Before we begin, I just want to confirm that you've had a chance to read and sign the Informed Consent Form (ICF).
 - Have you received it?
 - And have you signed it? (If yes → proceed.) (If no → pause to sign.)
- **Interviewer:** Perfect — thank you. Just as a quick reminder, everything you share today will be anonymised, and you can skip any question or stop at any time. The interview should take about 45–60 minutes. Does that still work for you? (Wait for confirmation.)

2. Short Introduction & Purpose

Interviewer: [Introduce myself briefly.]

To give a bit of context: this interview is part of my Master's thesis, which explores strategies for driving the adoption of digital identity wallets. I'm interested in your experience with digital identity systems and in hearing what you think works — or doesn't — when encouraging adoption by end-users.

There are no right or wrong answers — I'm mainly looking to understand your perspective and experience. (Pause to let this land.)

3. Warm-Up: Background & Expertise

Interviewer: To get us started more gently, I'd like to ask a few background questions just so I understand your experience and the context you are working in.

1. Could you briefly describe your role and how it connects to digital identity or wallet initiatives—for example, the products, projects, or ecosystems you have worked on or helped design or launch?
2. What was your organisation's role in those initiatives (e.g., provider, orchestrator, regulator, relying party, integrator)?
3. (From your perspective, what does "successful adoption" mean in digital identity ecosystems?)

(These warm-up questions establish credibility and get the expert talking comfortably.)

4. Main Interview Questions

Section 1 — Strategic Thinking & Decision-Making

Goal: Understand how they think strategically and how they approached adoption challenges.

1. When you think back to the [digital identity or wallet initiative(s)] you worked on, what were the core strategic objectives guiding adoption?
2. What were the biggest strategic dilemmas you faced early on?
e.g., users vs. RPs, trust vs. usability, speed vs. security
3. How did you prioritise different adoption challenges?
Probe: What trade-offs did you consciously make?

Section 2 — Strategies That Were Actually Used

Goal: Get real concrete strategies that were applied — not abstract opinions.

4. What specific strategies did your team use to drive adoption by end-users?
Examples: piggybacking, marquee partners, micro-market pilots, seeding, incentives, UX redesigns, trust-building campaigns
5. Which of those strategies worked best, and why do you think they worked?
6. Which strategies failed or underperformed? Why?
Probe hard here: Look for organisational blockers, misalignment, poor timing, wrong target group, etc.
7. Were there strategies you wish you had used earlier? Or avoided?

Section 3 — Trust Strategies (if any)

8. What trust-building strategies did you use to encourage uptake?
Trust anchors, partnerships, certifications, transparency measures
9. Which trust-building actions had the greatest impact?
10. Where did trust strategies fail or backfire?

Section 4 — Value Proposition & Use Case Strategies (if needed)

11. How did you decide which use cases to launch with?
12. What strategies did you use to communicate user value early on?
13. Were there use cases you expected to drive adoption but didn't? Why?
14. Looking back, which use case choices were strategically decisive?
15. *New Question added after Interview 1: Have you considered implementing age verification (AV) as a specific use case within your digital identity wallet or solution? If so, how was it positioned strategically? If not, what factors influenced the decision not to pursue it?*
(This question was added after the first interview to ensure systematic coverage of age verification as a potential wallet use case.)

Section 5 — Relying-Party (RP) Integration Strategies (won't get to this, unless they do)

16. What strategies did you use to onboard RPs?
Technical toolkits, integration support, incentives, sandbox availability, co-design, regulatory push
17. What were the biggest mistakes or obstacles in RP onboarding?
18. Which strategies, if any, were especially effective in convincing RPs to join early?

Section 6 — Network Effects & Critical Mass Strategies (if needed)

Targeting the chicken-and-egg problem explicitly.

19. How did you approach the chicken-and-egg problem?
Users first? RPs first? Both? Something else?
20. Did you use strategies like piggybacking, micro-market launching, seeding, or marquee customers? How effective were they?
21. What conditions helped your ecosystem reach or approach critical mass?
22. Where did network effect strategies fail, stall, or not behave as expected?

Section 7 — Incentive Strategies (if needed)

23. Did you use financial or non-financial incentives for users or RPs?
24. Which incentive tactics worked? Which didn't?
25. Did incentives create any unintended consequences or dependencies?

Section 8 — UX & Communication Strategies (won't get to this, unless they do)

26. What UX or communication strategies were used to drive adoption?
27. Which UX decisions had strategic importance?
28. Did user education campaigns or communication strategies matter?

Section 9 — Governance & Orchestration Strategies (if needed)

29. What governance or coordination strategies influenced adoption?
30. What strategic misalignments (between actors) created adoption barriers?
31. What governance approaches helped the ecosystem move forward?

Section 10 — Strategic Lessons Learned

32. What were the biggest strategic lessons you learned about driving the adoption of digital identity wallets or similar systems?
33. If you were to launch a digital identity (wallet) again, which strategies would you prioritise?
34. Which strategies would you avoid?
35. What do you see as the biggest strategic risk for the EU Digital Identity Wallet?
36. What opportunities are being overlooked?

Section 11: Additional Final Question (Dutch Wallet Context) (if applicable)

Interviewer: One last question, specifically regarding the Dutch digital identity landscape. As you might know, the government intends to release its own wallet first and then allow private wallet providers to enter the market afterwards.

From your perspective, what is your strategic response to this sequencing?

- How do you see your organisation positioning itself once private providers are allowed in?
- And what strategies do you think will be necessary to compete or differentiate in a market where the government wallet launches first?
- What opportunities or risks do you anticipate?

5. Closing

37. Is there anything else strategic about adoption that we haven't discussed but you consider important?

Interviewer: Before we wrap up:

Given your experience in this area:

Do you think there is anyone else — either within your organisation or in your wider professional network — who would also be a good fit for this study and open to being interviewed?

(Pause and let them think.)

...It could be someone who worked on digital identity strategy, wallet implementation, relying-party onboarding, regulatory aspects, or ecosystem coordination. I'd really appreciate any recommendations.

Before we finish, I also wanted to mention that once the interview is transcribed (as in the ICF stated), I will send you an anonymised version of the transcript. You'll have the opportunity to review it and make any corrections or clarifications you feel are necessary.

Thank you a lot for your time and insights, very helpful!

8.3.2 Interview Guide – Age Verification Experts

Note: Text in **colour** highlights wording that was adapted specifically for the age-verification (AV) interview guide.

Semi-Structured Interview Guide – AV Experts

0. Opening & Warm-Up

- **Interviewer:** Hi, thanks so much for taking the time to speak with me today. Before we start, how are you doing?
- **Interviewer:** Great — thanks again for participating. I really appreciate your willingness to share your experience.

1. Informed Consent Check

- **Interviewer:** Before we begin, I just want to confirm that you’ve had a chance to read and sign the Informed Consent Form (ICF).
 - Have you received it?
 - And have you signed it? (If yes → proceed.) (If no → pause to sign.)
- **Interviewer:** Perfect — thank you. Just as a quick reminder, everything you share today will be anonymised, and you can skip any question or stop at any time. The interview should take about 45–60 minutes. Does that still work for you? (Wait for confirmation.)

2. Short Introduction & Purpose

Interviewer: [Introduce myself briefly.]

To give a bit of context: this interview is part of my Master’s thesis, which explores strategies for driving the adoption of digital identity wallets, **with a specific focus on age verification as an early use case. I’m interested in your experience with age-verification initiatives** and in hearing what you think works — or doesn’t — when encouraging adoption by end-users. **This case is particularly interesting due to the 2-sided market and chicken-egg-problem arising.**

There are no right or wrong answers — I’m mainly looking to understand your perspective and experience. (Pause to let this land.)

3. Warm-Up: Background & Expertise

Interviewer: To get us started more gently, I’d like to ask a few background questions just so I understand your experience and the context you are working in.

1. Could you briefly describe your role and **how it connects to age-verification initiatives?**
2. What was your organisation’s role in those initiatives (e.g., provider, orchestrator, regulator, relying party, integrator)?
3. (From your perspective, what does “successful adoption” look like for **age verification solutions?**)

(These warm-up questions establish credibility and get the expert talking comfortably.)

4. Main Interview Questions

Section 1 — Strategic Thinking & Decision-Making in AV

Goal: Understand how they think strategically and how they approached adoption challenges.

1. When you think back to your work with digital identity **or age verification**, what were the core strategic objectives guiding adoption?
2. What were the biggest strategic dilemmas you faced early on?
e.g., privacy vs compliance, minors vs adults, UX vs security
3. **How did you prioritise adoption challenges for: users? relying parties (RPs)?**
Probe: What trade-offs did you consciously make?

Section 2 — Strategies That Were Actually Used

Goal: Get real concrete strategies that were applied — not abstract opinions.

4. What specific strategies did your team use to drive adoption by end-users?
Examples: piggybacking, marquee partners, micro-market pilots, seeding, incentives, UX redesigns, trust-building campaigns
5. Which of those strategies worked best, and why do you think they worked?
6. Which strategies failed or underperformed? Why?
Probe hard here: Look for organisational blockers, misalignment, poor timing, wrong target group, etc.

7. Were there strategies you wish you had used earlier? Or avoided?

Section 3 — Trust Strategies (if any)

8. What trust-building strategies did you use to encourage uptake?
Trust anchors, partnerships, certifications, transparency measures
9. Which trust-building actions had the greatest impact?
10. Where did trust strategies fail or backfire?

Section 4 — Value Proposition & Use Case Strategies (if needed)

11. How did you decide which **age-restricted** use cases to launch with?
12. What strategies did you use to communicate user value early on?
13. Were there use cases you expected to drive adoption but didn't? Why?
14. Looking back, which use case choices were strategically decisive?

Section 5 — Relying-Party (RP) Integration Strategies (won't get to this, unless they do)

15. What strategies did you use to onboard RPs?
Technical toolkits, integration support, incentives, sandbox availability, co-design, regulatory push
16. What were the biggest mistakes or obstacles in RP onboarding?
17. Which strategies, if any, were especially effective in convincing RPs to join early?

Section 6 — Network Effects & Critical Mass Strategies (if needed)

Targeting the chicken-and-egg problem explicitly.

18. How did you approach the chicken-and-egg problem?
Users first? RPs first? Both? Something else?
19. Did you use strategies like piggybacking, micro-market launching, seeding, or marquee customers? How effective were they?
20. What conditions helped your ecosystem reach or approach critical mass?
21. Where did network effect strategies fail, stall, or not behave as expected?

Section 7 — Incentive Strategies (if needed)

22. Did you use financial or non-financial incentives for users or RPs?
23. Which incentive tactics worked? Which didn't?
24. Did incentives create any unintended consequences or dependencies?

Section 8 — UX & Communication Strategies (won't get to this, unless they do)

25. What UX or communication strategies were used to drive adoption?
26. Which UX decisions had strategic importance?
27. Did user education campaigns or communication strategies matter?

Section 9 — Governance & Orchestration Strategies (if needed)

28. What governance or coordination strategies influenced adoption?
29. What strategic misalignments (between actors) created adoption barriers?
30. What governance approaches helped the ecosystem move forward?

Section 10 — Strategic Lessons Learned

31. What were the biggest strategic lessons you learned about driving the adoption of **age verification solutions**?
32. If you were to launch an **age verification** wallet/app again, which strategies would you prioritise?
33. Which strategies would you avoid?
34. What do you see as the biggest strategic risk for the EU Digital Identity Wallet?
35. What opportunities are being overlooked?

Section 11: Additional Final Question (Dutch Wallet Context) (if applicable)

Interviewer: One last question, specifically regarding the Dutch digital identity landscape. As you might know, the government intends to release its own wallet first and then allow private wallet providers to enter the market afterwards.

From your perspective, what is your strategic response to this sequencing?

- How do you see your organisation positioning itself once private providers are allowed in?
- And what strategies do you think will be necessary to compete or differentiate in a market where the government wallet launches first?
- What opportunities or risks do you anticipate?

5. Closing

36. Is there anything else strategic about adoption that we haven't discussed but you consider important?

Interviewer: Before we wrap up:
Given your experience in this area:

Do you think there is anyone else — either within your organisation or in your wider professional network — who would also be a good fit for this study and open to being interviewed?

(Pause and let them think.)

...It could be someone who worked on digital identity strategy, wallet implementation, relying-party onboarding, regulatory aspects, or ecosystem coordination, or age verification. I'd really appreciate any recommendations.

Before we finish, I also wanted to mention that once the interview is transcribed (as in the ICF stated), I will send you an anonymised version of the transcript. You'll have the opportunity to review it and make any corrections or clarifications you feel are necessary.

Thank you a lot for your time and insights, very helpful!

8.4 Informed Consent Form (ICF)

The following pages contain the Informed Consent Form (ICF) approved by the Human Research Ethics Committee (HREC). The document below is included in its original format to preserve the exact wording provided to participants.

Participant Information

Study title: Adoption of Wallet-Based Age Verification in the European Union

Researcher: Ir. Magda Lamprinidou, Master's student (MSc Management of Technology), Faculty of Technology, Policy and Management, Delft University of Technology (TU Delft)

Supervisor: Prof.dr.ir. Mark de Reuver, TU Delft

Host organisation: INNOPAY, a division of Oliver Wyman B.V.

Purpose of the study:

This research explores adoption strategies for digital identity wallets, focusing on the voluntary, platform-dependent use case of age verification (AV). The study aims to identify best practices and challenges from prior digital identity initiatives and to understand expert perspectives on future wallet adoption. The main research question of this study is *“What adoption strategies could wallet providers consider when rolling out digital identity wallets?”*.

What participation involves:

If you agree to participate, you will be asked to take part in an interview lasting approximately 45–60 minutes. The interview will be recorded (with your consent, below) and later transcribed. The researcher will take notes and use anonymised excerpts to analyse themes across all interviews.

Risks and benefits:

There are no physical, psychological, or financial risks associated with participating in this study. However, since the research involves discussing professional experiences and opinions within the digital identity (and age-verification domain, if applicable), there is a small potential risk that participants could be indirectly identifiable based on their role, organisation, or project involvement.

To mitigate this risk, you will be assigned a random identifier and the transcripts will be anonymized to the extent possible, meaning all identifying information (such as names, organisations, and specific project references) will be removed or generalised during the data aggregation process.

You will receive the aggregated/anonymised transcript for review and approval. Upon consent, the aggregated/anonymized data will be used for the analysis, and only anonymised data will be used in reports and/or publications.

There are no direct personal benefits for participants, but your insights will contribute to a better understanding of how digital identity wallets and age-verification solutions could be effectively adopted and governed across Europe.

After the study is completed, participants will be offered a copy of the final Master's thesis and presentation materials.

Confidentiality and data protection:

- Interview recordings will be securely stored on a restricted-access TU Delft network drive accessible only TU Delft Supervisor.

Informed Consent Form – MSc Thesis, TU Delft

- All interview data will be anonymised before analysis and any form of sharing. This means that your name, company, and any other directly identifying details will be masked, removed or coded. Indirect identifiers (such as specific projects, unique job titles, or detailed organisational references) will also be generalised or omitted. For example: Instead of *“John Doe, Senior Digital Identity Consultant at Innopay, 7 years of work experience”* the anonymised transcript might read *“Interviewee #A3b14, senior consultant in digital identity (5–10 years of professional experience).”* And Instead of *“Worked on the UK Age Verification pilot with major online retailers,”* it might read *“involved in a national age-verification initiative for online platforms”*. This process ensures that neither you nor your organisation can be identified in any transcripts, analyses, or research publications.
- Participants will receive their aggregated/anonymised transcript for review and approval with a 2 weeks timeframe, after which if there is no response from the participant, it will be considered as an approval.
- The recordings will be deleted after transcription verification and this thesis completion.
- Only the aggregated/anonymised transcripts will be stored for future research in a restricted-access TU Delft network drive as mentioned before, and these transcripts will **not** be published as open data after the thesis completion.

Use of quotes: You may be quoted anonymously in research outputs. Explicit permission for the use of anonymised quotes will be requested below.

Voluntary participation: Your participation is voluntary, and you may refuse to answer any question or withdraw at any time without giving a reason. Withdrawal will not affect your relationship with TU Delft nor with INNOPAY.

Contact:

Researcher: Magda Lamprinidou

Thesis Academic Supervisor: Prof.dr.ir. G.A. Mark de Reuver, TU Delft

Explicit Consent points

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
A: GENERAL AGREEMENT – RESEARCH GOALS, PARTICIPANT TASKS AND VOLUNTARY PARTICIPATION		
1. I have read and understood the study information dated [DD/MM/YYYY], or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	☐	☐
2. I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	☐	☐
3. I agree that the interview may be audio-recorded for transcription purposes.	☐	☐

Informed Consent Form – MSc Thesis, TU Delft

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
4. I understand that the audio recording will be deleted after the aggregated/anonymised transcript is verified and the thesis is completed.	☐	☐
5. I agree that anonymised excerpts or quotes from my interview may be used in the thesis or related publications.	☐	☐
6. I understand that I will receive my aggregated/anonymised transcript and have two weeks to request corrections or redactions. If I do not respond within this period, the transcript will be considered approved for use in the research.	☐	☐
7. I understand that anonymised transcripts will be stored securely at TU Delft and may be used for future academic research carried out within the group of Dr. Mark de Reuver.	☐	☐
8. I understand that my personal information (name, email) will only be used for communication and consent documentation and will not appear in any publication.	☐	☐
9. I understand that the study will end upon completion of the researcher's Master's thesis at TU Delft, expected in March 2026. Also, I understand that: If unforeseen circumstances require an extension (for example, delays in thesis submission or defence), the study period may be extended accordingly, but no later than December 2026 . After the thesis is submitted and evaluated, all audio recordings and raw (non-anonymised) transcripts will be permanently deleted. Only aggregated/anonymised transcripts will be retained securely on a restricted-access TU Delft network drive for potential future academic research and publication.	☐	☐
B: POTENTIAL RISKS OF PARTICIPATING (INCLUDING DATA PROTECTION)		
10. I understand that taking part in the study involves the following risks: There are minimal risks associated with participating in this study. The primary risk relates to professional reputation, as interviews concern organisational practices and opinions. I understand that these will be mitigated by offering participants anonymity to the extent possible, removing or generalising any identifying information (e.g., names, organisations, or specific project references), and by allowing participants to review and approve their aggregated/anonymised transcripts before analysis.	☐	☐
11. I understand that taking part in the study also involves collecting specific personally identifiable information (PII): name and email address (for scheduling and communication purposes only) and associated personally identifiable research data (PIRD): professional role, domain of expertise, company type, and approximate years of experience (in ranges, e.g., "5–10 years"). Because participants are professionals in specialised domains, there is a risk of indirect re-identification. This will be mitigated through careful data aggregation/anonymisation and removal of organisational or project-specific details.	☐	☐

Informed Consent Form – MSc Thesis, TU Delft

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
12. I understand that this research does not involve the collection or processing of special categories of sensitive data as defined under GDPR (e.g., political opinions, religious beliefs, health data, or criminal records).	☐	☐
13. I understand that the following steps will be taken to minimise the threat of a data breach, and protect my identity in the event of such a breach. Data protection measures include: (1) storing all digital files on TU Delft's network with restricted access; (2) deleting audio recordings after transcript verification; (3) aggregating and anonymising all research data to the extent possible before analysis; (4) limiting access to aggregated/anonymised transcripts to the researcher and TU Delft academic supervisor during the master thesis project; limiting access to aggregated/anonymised transcripts to the TU Delft academic supervisor for the long-term (10 years).	☐	☐
14. I understand that personal information such as my name and email address will not be shared beyond the study team and will not appear in any publication or report.	☐	☐
15. I understand that the (identifiable) personal data I provide (such as names, email addresses, and audio recordings) will be destroyed after the aggregated/anonymised transcripts have been reviewed and approved by participants, and no later than the completion of the Master's thesis project.	☐	☐
16. I understand the signed informed consent forms will be stored for the long-term in a restricted-access TU Delft network drive, accessible to TU Delft Supervisor.	☐	☐
C: RESEARCH PUBLICATION, DISSEMINATION AND APPLICATION		
17. I understand that after the research study the de-identified information (anonymised transcripts) I provide will be used to develop the research findings for inclusion in the Master's thesis, academic presentations, and potential future journal publications.	☐	☐
18. I agree that my responses, views, or other input can be quoted anonymously in research outputs (e.g., Master's thesis, presentations, publications).	☐	☐
D: (LONGTERM) DATA STORAGE, ACCESS AND REUSE		
19. I give permission for the aggregated/anonymised interview transcripts to be stored on a restricted-access TU Delft network drive for potential future academic research. These data will not be shared publicly nor made openly accessible.	☐	☐
20. I understand that access to the aggregated/anonymised data will be restricted to the TU Delft Supervisor. The data will remain in anonymised form, and no commercial nor public access will be granted. - A summary of aggregated and anonymised research findings (for example, themes, frameworks, or non-identifiable illustrative quotes) may be shared with the host organisation for internal knowledge sharing or validation of insights. - The host organisation will not have access to any raw data, identifiable information, nor any individual transcripts; and no participant or organisation will be identifiable in any shared material.	☐	☐

Informed Consent Form – MSc Thesis, TU Delft

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
- Data will be retained for at least 10 years in line with TU Delft's Research Data Framework Policy.		

Signatures

Name of participant Signature Date

I, as legal representative, have witnessed the accurate reading of the consent form with the potential participant and the individual has had the opportunity to ask questions. I confirm that the individual has given consent freely.

Name of witness Signature Date

I, as researcher, have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.

Magda Lamprinidou

Researcher name Signature Date