LUISS

Degree Program in Data Science and Management

Course of Data Privacy and Security

Digital Identity Systems across diverse socio-economic landscapes A contingency approach

Prof. Paolo Spagnoletti

SUPERVISOR

Prof. Emilio Coppa

CO-SUPERVISOR

Claudia Compagnone Matr. 7

CANDIDATE

Academic Year 2023/2024

Table of Contents

ABSTRACT

This thesis highlights the importance of digital identity as enabler of secure and efficient transactions in the digital age, highlighting the challenges posed by the current fragmentation of digital identity systems in Europe and the complexities of Secure Customer Authentication processes, preventing in particular the full realization of Open Banking and, more broadly, Open Finance frameworks.

It starts by critically examining the evolution of digital identity frameworks in the European Union, from the establishment of the eIDAS regulation to its ongoing revision and the introduction of the European Digital Identity Wallet, and then explores the transformative potential of this tool, focusing on how it could enhance the banking and financial sector's efficiency, inclusivity, and competitiveness.

By conducting a comparative analysis of diverse national approaches to digital identity, this thesis investigates the alignment of digital identity systems with the socio-economic and institutional frameworks of different countries, aiming to develop a contingency theory that guides the implementation of these systems in diverse contexts.

INTRODUCTION

The Open Banking and Open Finance movements in Europe represent a fundamental shift in the financial sector, aiming to break down traditional banking monopolies on customer data and payment services. This shift has been driven by several factors, mainly technological advancements, regulatory changes like the Payment Services Directive 2 (PSD2), and the advent of digital platforms.
Since the adoption of PSD2 in 2018, Open Banking, primarily focusing on payment accounts, has been seeking to enhance competition and innovation in payments; more recently it has expanded into Open Finance, which covers a broader range of financial services including savings, investments, pensions, and insurance, offering consumers more control over their financial data and access to personalized services.

Despite the valid premises and the optimistic vision, a significant barrier in the practical implementation of Open Banking and Open Finance has turned out to be the fragmentation and inconsistency of digital identity systems across the EU, alongside complex Secure Customer Authentication (SCA) processes: the current landscape, characterized by a multitude of national digital identity initiatives and disparate SCA methods developed by banks, threatens the seamless cross-border use of digital IDs and detracts from user experience, ultimately limiting the adoption and growth of Open Banking and Open Finance solutions.

Regulatory intervention and harmonization efforts, such as the ongoing revision of the eIDAS regulation and the introduction of the European Digital Identity Wallet (EUDIW), are critical to overcoming these challenges: these efforts aim to streamline digital identity and SCA processes, trying to balance security and smoothness of digital interactions across the EU on one side, and supporting the growth and effectiveness of the Open Banking and Open Finance ecosystems on the other.

The thesis is structured as follows:

- Chapter 1 outlines the evolution of Open Banking and Open Finance in Europe, highlighting their potential to redefine financial services through enhanced access to financial data and a broader range of services. It explores the regulatory enablers of these revolutions, such as the PSD2 and the European Commission's subsequent initiatives aimed at fostering a secure, innovative, and competitive financial ecosystem, and the challenges posed by the fragmentation of digital identity systems and the complexities of SCA processes, underscoring the need for harmonization and simplification to realize the full potential.
- Chapter 2 lays the foundation for understanding the implications of digital identity developments on Open Banking and Open Finance by providing a comprehensive overview on the evolution of digital identity frameworks within the EU, from the introduction of eIDAS 1.0 to the changes brought by eIDAS 2.0 and the EUDIW.
- Chapter 3 conducts a literature review that synthesizes current academic discussions on the design, challenges, and potentials of digital identity wallets, while also highlighting significant gaps in how these systems are integrated with socio-economic structures across different countries. This review sets the foundation for introducing a novel contingent approach to understanding digital identity systems, which suggests that the effectiveness of such systems is contingent on the specific socio-economic and institutional contexts of each country. Following this, the chapter articulates a research question focused on how certain digital identity systems align with and succeed within their respective socio-economic environments.
- Chapter 4 outlines the methodology employed to answer the identified research question. This chapter details a comparative study of selected cases that demonstrate distinct approaches to digital identity management across different socio-economic and institutional environments, such as Estonia’s eID, Sweden’s BankID, India’s Aadhaar, and Singapore’s SingPass. The methodology section describes the collection of data from secondary sources to maximize comparability and efficiency and explains the structured thematic analysis used to systematically examine and identify key features and patterns within these systems.

- Chapter 5 conducts an analysis of socio-economic contexts and digital identity systems across the selected countries and a thematic analysis along the dimensions of trust establishment, credential sharing management and widespread accessibility insurance, examining how each aligns with its socio-economic context. Through thematic analysis, it identifies key features contributing to each system's success (e.g., government initiative, technological integration, public-private collaboration…). The findings inform the development of a contingency theory that links specific digital identity features to socio-economic frameworks, proposing adaptable models for countries with similar contexts.
- Finally, chapter 6 synthesizes the findings, addressing the research question. It outlines key insights from the analysis, discusses theoretical and practical implications and acknowledges research limitations as well. The chapter concludes by suggesting future research directions to explore broader digital identity applications and additional socio-economic environments.

Through the analysis of international experiences and best practices, this thesis aim overall is to offer valuable insights for policymakers, financial institutions, and technology providers working at the forefront of digital transformation in the financial sector.

CHAPTER 1: CHALLENGES IN THE IMPLEMENTATION OF OPEN BANKING AND OPEN FINANCE SOLUTIONS: FOCUS ON THE FRAGMENTATION OF DIGITAL IDENTITY SYSTEMS

1.1 The Open Banking and Open Finance revolution in Europe

The digital economy, relating to economic activity that results from using digital technology to connect individuals, businesses, processes, devices and data, is one of Europe's main sources of growth. Technological advances, new players and their ground-breaking business models, and shifting consumer behaviour have already sped up structural transformation in the financial sector: this, in fact, is becoming increasingly decentralised and several non-bank forms of credit are emerging; as competition intensifies and more and more specialised financial solutions are introduced, customer welfare could considerably increase.
For this transformative process to be successful, some of the fundamental aspects to be taken care of are data access and a sound legal framework for data sharing.

The advent of Open Banking and Open Finance in Europe represents a paradigm shift in the financial services sector, driven by digital innovation and legal changes. Fundamentally, these frameworks seek to break up the established banking industry's monopoly on payment services and customer data, creating an environment that is more open to competition, innovation, and consumer choice. The premise is simple but transformative: they aim to give the possibility to consumers to securely share their financial data with third-party providers (TPPs) through Application Programming Interfaces (APIs), thus facilitating the market entry of new and innovative players and enabling a wide range of customised financial services.
Open Banking initially focused solely on payment accounts, in order to promote competition and innovation in the payment industry; however, the vision has quickly

expanded into Open Finance, affecting a broader range of financial services, including savings, investments, pensions, and insurance. This evolution offers consumers unparalleled control over their financial data and access to a wide range of services tailored to their specific needs, promising a more holistic approach to financial management.

The establishment of Open Banking in Europe is closely tied to the digital transformation, marked by the rise of digital platforms and the increasingly widespread use of mobile and digital technologies that have impacted almost every industry, finance included. The Payment Services Directive 2 (PSD2 hereinafter) is a regulation adopted by the European Union with the aim to drive innovation, competition, and enhance transparency in the banking sector and has significantly impacted the financial services industry (The European Parliament and the Council of the European Union, 2015).

The PSD2 directive, effective from January 2018, mandated banks to open access to their customer data and payment services to TPPs through APIs, dramatically altering the well-established banking ecosystem. By embracing the principles of openness and cooperation, the directive allowed new players, such as technology startups and digital native financial organisations, to join the traditionally guarded and heavily regulated industry and offer new technologies, services and way of doing business. It effectively shattered the comfortable and stable status-quo and opened the financial services industry.

An illustrative case of this digital transformation is Flowe, an Italian startup owned by Gruppo Mediolanum, established in 2020 in the middle of the global pandemic. Despite this, Flowe has rapidly captured a considerable user base of more than 670,000 people and established partnerships with over 50 entities. It leverages open banking principles to offer payment solutions, while simultaneously promoting environmental consciousness and financial education through gamified experiences (Kallinikos et Al., 2022).

The success of Flowe encapsulates the essence of the fintech revolution encouraged by PSD2, that has seen the emergence of a new industry practice characterized by the application of internet technologies, cloud computing, and mobile devices to deliver a range of financial services, from mobile payments to investment management. These fintech entities stand out for their disruptive potential, initiating new services, business models, and collaborative practices.

The open banking initiative, initiated by PSD2, has facilitated the sharing of financial data across the ecosystem, supporting innovation and the provision of tailored financial solutions. This trend towards openness and technological integration marks a fundamental change from the traditional vertically integrated banking models towards a platform-based ecosystem, where value creation is increasingly externalized and managed through digital platforms and APIs. This ecosystem approach not only facilitates innovative service offerings but also inspires a culture of collaboration and data sharing, consequently enhancing consumer choice, promoting competition, and making a more inclusive and dynamic financial services sector possible.

Open Finance aims to further expand the scope of Open Banking, by including mortgages, insurance, pensions, and investment services in addition to payment accounts: this could allow customers to have a single point of access and to simplify typically long and complicated processes such as access to loans, comparison of offers from banks, insurance companies and much more. All of this could be enabled by advanced data analysis of aggregated information on all banking or more generally financial functionalities needed to operate daily, including information on savings and expenses of different bank accounts. This trend is rapidly spreading, driven by the collaboration between regulators, standardization initiatives advocates, market players (traditional banks, digital banks and fintechs) and end consumers, all of them contributing to the "Open" ecosystem.

The European Commission (EC) is working to expand the innovations introduced by the PSD2 directive in the field of Open Banking pushing in the direction of Open Finance, launching new initiatives including the Digital Finance Package[1], the Open Finance Consultation[2] and the EU Data Act[3]. The goal is to enhance data-sharing-based business

[1] The Digital Finance Package is a set of legislative measures that define how the EU can support the digital transformation and innovation of the financial sector, including significant actions in the areas of Digital Identity, Open Finance, Crypto-assets, Digital Resilience, Blockchain and consumer protection.

[2] The Open Finance Consultation is a targeted public consultation launched by the Commission to collect market feedback on the application and impact of PSD2 and Open Finance opinions.

[3] The European Data Act is a proposed regulation of a harmonised framework for data sharing in the European Union. This law will increase the amount of data available for use and establish guidelines for access, management and purposes in all EU economic sectors.

models and services, starting with the payments industry, consequently facilitating and preparing the application of the same principles in other industries.
Additionally, the EC has evaluated the benefits and drawbacks of the current Open Banking system established by PSD2 and has developed reasonable plans to broaden it: on June, the 28th 2023 new regulations and directives have been proposed to define a reliable Open Finance framework within the EU, specifically the Third Payment Services Directive (PSD3) and the Payment Services Regulation (PSR) as an evolution of the existing legal acquis of PSD2, that together form the "Payments Package", and the complementary Financial Data Access Regulation (FiDA) aiming to regulate the access, sharing and use of customer data in the financial sector, thus covering financial services and accounts which were not covered by PSD2.

As Europe advances toward realizing the full potential of Open Banking and Open Finance, an emerging challenge demands attention: the rising dominance of Big Tech companies (such as Google, Apple, Facebook and Amazon) in the financial sector. These tech giants, with their extensive technological expertise and global consumer reach, pose a significant threat to traditional banking structures and the nascent Open Finance ecosystem. Their incursion into financial services, ranging from digital wallets to lending, requires a remarkable effort by European regulators for the preservation of the competitive landscape, protection of consumer data, and the safeguarding of European financial sovereignty, and highlights the need for innovations in the EU banking space, not only as measures to enhance consumer choice and financial inclusivity, but also as strategic imperatives to counter the increasing influence of Big Techs and retain banks and financial institutions' relevance in the future. Such actions are essential to ensure that the European financial sector remains robust, competitive, and aligned with the stringent data privacy and security standards laid down by European law.

Once clarified the reasons why it is in everyone's interest in Europe to make this system work, before we figure out how to make Open Finance framework properly function, we should identify areas that are still controversial within the Open Banking experience. In fact, Open Banking in EU has not yet reached its full potential since the entry into force of the PSD2 in 2018, and a major impediment to its effectiveness has been the lack of

consistent standards, in particular within the electronic identification and trust services, that led to cumbersome authentication processes and subsequently a low services adoption rate.

At the heart of this revolution lies the concept of digital identity, serving as the backbone for secure and efficient transactions. Digital identification solutions that are trustworthy for distant customer authentication are becoming more and more important as financial services gradually move away from traditional face-to-face business and into the digital setting. The concept of digital identity covers a broad range of aspects from security and ethics, to technology and user experience. In addition to making it easier for people to be identified and authenticated in digital settings, digital identity serves as the foundation for all transactions and data exchanges within the Open Banking ecosystem. Complementing this, PSD2 has introduced Secure Customer Authentication (SCA) requirements, that ensure that transactions are performed securely, from the access to payment accounts to the initiation of digital payments, mitigating the risk of fraud and enhancing consumer trust in digital financial services.

Digital identity systems have the potential to fundamentally transform the landscape of financial services, driving innovation and enhancing the efficiency of processes such as payments, lending, and customer onboarding: by leveraging digital identity verification, financial institutions and fintech companies can offer more seamless and user-friendly experiences, while also strengthening security and trust during digital transactions.

Let’s consider an example that illustrates the transformative impact of digital identity systems on financial services: applying for a bank loan. Traditionally, applying for a bank loan is a cumbersome process involving multiple in-person meetings, extensive paperwork, and a significant time commitment from the applicant. However, thanks to a proper digital identity system, applicants could streamline this process significantly: users could simply select the necessary documents stored in their digital wallet and securely send verifiable digital documents to the bank for verification. This not only simplifies the application process but also reduces the time and resources spent by both the bank and the applicant, proving the power of digital identity systems in alleviating financial services and make them accessible to everyone.

Electronic identification schemes have been created in several EU Member States for customer authentication based on national electronic identification solutions that provide the greatest levels of assurance. Nonetheless, the EU landscape is currently charaterized by a wide range of different authentication solutions at national level with little cross-border interoperability, that could impede the creation of new payment services and additional innovation.

The European financial sector has always stood at a crossroads between market-driven innovation and the need for regulatory oversight, and we can clearly see it in the context under analysis.

On one hand, the EC has pushed for Open Banking and Open Finance through regulatory requirements such as PSD2 to ensure a unified vision and direction for the technology's development across Member States. This has indeed opened the doors to unprecedented levels of innovation, competition, and consumer choice.

Confirming its leadership in digital regulation, Europe has accompanied the advent of PSD2 with significant interventions in adjacent digital sectors. In the migration period foreseen by the Directive (1/2018 - 9/2019) the regulations on data protection and data reporting (GDPR and MIFID II) came into force, and at the same time the cross-border recognition of the trust services provided by the eIDAS Regulation in the field of digital signatures and identities has been launched.

Within a period of just over a year, the market has seen the deployment of four regulations relating to digital services, each with its own characteristics and goals, which together have given a strong impetus to the digitization of financial services, with important repercussions also on other market areas.

On the other side, the absence of union-wide standards, including for digital identity and authentication processes, has led to a fragmented market both across EU and within single Member States, ultimately resulting in an overall less than hoped take-up of services.

This fragmentation not only suppress innovation but also poses risks to consumer privacy and data security: the challenge lies in balancing the need for innovation with the imperative for robust security measures and consumer protections.

Moreover, the absence of sector-wide standards will further encourage tech giants, to stand in and dominate even the user identity landscape, simplifying the identification path

for users, but also collecting highly sensitive information of EU citizens and businesses: the EU should absolutely provide a safer and more trustworthy alternative, which complies with the rules of the continent in terms of data privacy and security.

The development and harmonization of digital identity frameworks throughout Europe are central to the efforts that are being made, providing a secure and efficient foundation for the sharing and management of financial data. By reinforcing the digital infrastructure with coherent digital identity solutions, Europe can strenghten its financial institutions, TPPs, and the broader financial ecosystem against the challenges posed by Big Tech dominance, ensuring a financial landscape that is innovative, consumer-friendly, resilient and respectful of European regulatory values.

1.2 Fragmentation of Digital Identity systems and complexity of SCA processes

As just anticipated, despite the optimistic vision to increase competition, innovation, and consumer choice, in practice the implementation of Open Banking solutions has encountered significant obstacles, primarily arising from the fragmentation and inconsistency of digital identity systems across the European Union and the significant usability issues due to the disparate and non-standardized SCA processes developed by incumbent banks.

The European Union's approach to digital identity systems is characterized by a significant degree of fragmentation and inconsistency across its member states, resulting in a multitude of national digital identity initiatives, each with its own standards and protocols, rather than a unified, pan-European framework. This fragmentation is primarily due to the voluntary nature of the eIDAS Regulation on digital identity (The European Parliament and the Council of the European Union, 2014), that complements the additional functionality brought in by the PSD2: TPPs must interface with existing core banking systems to access relevant customer data and provide their services and eIDAS offers the resources required to fulfil security, authentication, and document verification requirements. Although this regulation permits the creation and use of digital

IDs, it does not require member states to create, notify, or mutually recognize national eID schemes. As a result, digital identity coverage extends to only about 60% of European citizens across 14 member states (European Commission, 2021), leaving a considerable portion of the EU population without access to digital ID services. This lack of uniformity not only prevents the cross-border use of digital IDs, thereby undermining the European Digital Single Market's potential, but also detracts from the overall competitiveness and digital sovereignty of the Union.

Moreover, although the implementation of SCA in the Open Banking sector is a cornerstone for ensuring security within digital financial services, it revealed significant usability issues due to the fragmented approaches taken by incumbent banks; in fact, they have been left to develop their own SCA processes, leading to a variety of lengthy and user-unfriendly methods. These processes, designed without a standardized framework, not only confuse consumers, that are required to navigate through numerous screens, but also detract from the overall user experience. This complexity has been criticized by both regulators and fintech executives, that accuse established financial institutions, which possess minimal incentive to simplify or unify these processes, of deliberately creating obstacles: such barriers are strategically placed to restrict fintechs' access to customer data, aiming to preserve incumbents' control over this information and limit interactions with TPPs. This approach complicates the consumer journey and threatens the acceptance and growth of Open Banking and Open Finance by adding avoidable complexity to the financial ecosystem.

These challenges underscore the need for regulatory intervention and a collaborative effort by all the involved actors to overcome the fragmentation of digital identity systems, streamline SCA processes, and facilitate seamless, secure cross-border digital interactions for EU citizens.
The European Union has been taking bold steps in the recent years towards harmonization and simplification through the ongoing revision of the eIDAS regulation and the upcoming introduction of the European Digital Identity Wallet.

CHAPTER 2: NAVIGATING THE EUROPEAN DIGITAL IDENTITY LANDSCAPE

This chapter aims to address both the historical context and the evolution of digital identity frameworks within the European Union, as well as the transition from eIDAS to eIDAS 2.0 and the introduction of the European Digital Identity Wallet (EUDIW). The goal is to contextualize the developments in digital identity regulation and technology and set a solid foundation for discussing the implications of these changes on Open Banking and Open Finance.

2.1 Importance of Digital Identity in today's society

In the age of rapid digitalization, digital identities have become an essential part of modern society, enabling safe access to a wide range of online services and transactions. The European Union, recognizing the critical role of digital identity, has implemented the eIDAS regulation to standardize electronic identification and trust services across member states: this regulatory framework is the evidence of the EU's commitment to enhancing the digital single market by ensuring secure and seamless digital interactions for its citizens and businesses.

The importance of digital identity extends far beyond the European context: in fact, the United Nations' Sustainable Development Goals (SDGs), particularly Target 16.9, highlight the global necessity of ensuring that everyone has access to legal identity by 2030. This ambition highlights the foundational role of identity in accessing essential services, participating in the digital economy, and exercising rights. In an era where countries are transitioning to e-government systems that need a digital identity to transact, the SDG of a legal identity for all translates into practice with a digital identity for all (Sullivan, 2018).

Figure 1: the 17 Sustainable Development Goals established in 2015 as part of the UN 2030 Agenda for Sustainable Development, with focus on target 16.9 - Provide Universal Legal Identity

According to World Bank estimates, 850 million people globally do not have basic identity credentials: this underscores the extent of financial exclusion and the obstacles that people face when attempting to obtain essential services like banking, insurance, and social protection (The World Bank Group, 2021). This exclusion not only impedes individual prosperity but also slows down economic development and social cohesion.

Digital identity systems offer a powerful tool to address these challenges; in fact, by transitioning to digital identification, countries can improve access to services, enhance data security, and reduce the risks of fraud and identity theft. The potential economic

benefits are substantial, with McKinsey estimating that digital identity could unlock value equivalent to 3-13 percent of GDP by 2030, percentage that would be even greater if we only considered emerging economies, where the potential for improvement is huge (McKinsey Global Institute, 2019).

The advent of digital identity wallets represents a significant innovation in identity management, replacing traditional methods of identification and authentication, that are more prone to fraud or theft: these wallets provide a secure and user-centric platform for managing digital identities, enabling individuals to control their personal data and how it is shared. This shift towards decentralized identity management offers several advantages, including enhanced security, increased privacy, and greater convenience for users that could store and access all their personal information in one place.
Digital identity wallets can streamline various processes, from onboarding for new services to verifying credentials, thus reducing administrative burdens and improving overall user experience.

The importance of digital identity in today's society cannot be overstated: it underlies the digital economy, supports the delivery of public and private services, and plays a crucial role in ensuring inclusive and widespread access to opportunities and rights. As digitalization continues to transform all aspects of life, the development and adoption of robust digital identity frameworks become essential for fostering economic growth, social inclusion, and the protection of fundamental rights.

2.2 A brief history of Digital Identities in the European Union

The development of digital identity in the European Union has proceeded through a significant evolution in regulatory frameworks and technological solutions, promoting secure electronic transactions and identity verification across Member States. This path, initiated in the late 90s, is marked by legislative milestones, innovative initiatives, focus on interoperability and security.

The foundation for digital identity in the EU was laid in 1999, with the adoption of the Directive on Electronic Signatures (The European Parliament and the Council of the European Union, 1999): for the first time, it provided a legal framework for electronic signatures, affirming their equality with written signatures from a legal point of view, in terms of validity and enforceability. This first piece of legislation, which well framed the EU recognition of the fundamental importance of digital identity in the emerging digital landscape, was a step towards the digitization of society and the related imperative of secure electronic transactions.

The desire of the EU to move towards a common framework for digital identity is also demonstrated by the start of the STORK (Secure idenTity acrOss boRders linKed) project in 2008, which aimed at developing an European interoperability platform for eID, so that citizens could use their national eIDs for cross-border electronic transactions (Elsevier, 2008). The STORK project was a fundamental step towards the creation of conditions for seamless digital interactions across the EU, underlining the role of interoperability in the framework of digital identity deployed in the Union.

The key step in the evolution of digital identities within the EU was the introduction of the eIDAS regulation in 2014, which replaced the Electronic Signatures Directive (The European Parliament and the Council of the European Union, 2014): eIDAS offers a regulatory framework for electronic identification and trust services, including electronic signatures, seals and time stamps, registered delivery services and website authentication certificates. Its goal is to provide a high level of convenience and security for all electronic transactions, through the establishment of a digital single market in the EU, characterized by interoperability and security.

In the following subsection we will explore the aforementioned Digital Single Market Strategy for Europe.

2.3 European Digital Single Market

The European Digital Single Market (EDSM henceforth) was established in 2015 as a significant development in the harmonisation of the digital economy across the Member States of the European Union (European Commission, 2015). The EDSM initiative seeks to eliminate fragmented digital markets within the EU and create a single market that facilitates the development, innovation and competitiveness of digital networks and services on an international scale.

AT its core, the EDSM is rooted in the fundmental concept of the EU's single market, which ensures the free movement of people, goods, services, and capital. In today's digital era, this principle extends to ensuring that digital services and goods move freely across borders, thus amplifying competition and enhancing Europe's attractiveness as a hub for investment. The EDSM agenda consists of three pillars: better access to digital goods and services; a better environment for digital networks and services; and using digitalisation as a driver to boost economic growth.

Integral to the EDSM are two critical pieces of legislation, namely the Digital Markets Act (DMA) and the Digital Services Act (DSA), both part of the broader Digital Services Act package.

The DMA intends to limit the power of large digital platforms, the so called "gatekeepers", to ensure that they do not act in ways that may harm competition and the ability of other market players to innovate. In this way, the DMA should boost consumer choice and enable start-ups to compete more effectively with major tech corporations (The European Parliament and the Council of the European Union, 2022 – a).

The DSA, often considered the DMA's counterpart, addresses the need to ensure a safer digital environment for its users, the protection of fundamental rights, and a fair and predictable field for businesses. It demands stricter transparency obligations and regulates targeted advertising and business user traceability (The European Parliament and the Council of the European Union, 2022 – b).

The EDSM envisions a seamlessly integrated European market where people can fully enjoy digital technologies and services without being hindered by cross-border barriers. Such integration should boost cross-border online transactions, spur investments in new online services and applications, and stimulate the development of digital infrastructures. Removing barriers to online activity should bring major economic benefits, including innovation-driven productivity gains across sectors, improved public sector efficiency, and enhanced consumer welfare through lower prices and greater choice.

2.4 The eIDAS Regulation

The regulation on Electronic Identification, Authentication and Trust Services (eIDAS) was originally approved by the European Union in 2014 and reviewed in recent years with the main objective to create the basis for secure electronic transactions within the EU and strengthen the digital single market. One of the main drivers of eIDAS was to reach mutual recognition of electronic IDs (eIDs) in the EU Member States and allow citizens and businesses to easily access online services across borders. The regulation covers various trust services, including electronic signatures, seals, time stamps, and document authentication, that are essential for secure digital transactions and interactions across the EU. By standardizing these trust services, eIDAS strengthened trust and security in the EU's digital economy.

With the revision of the original regulation, significant enhancements are introduced, particularly concerning the European Digital Identity Wallet.
Let’s now investigate further the innovations brought by the original eIDAS regulation (eIDAS 1.0 hereinafter), the impact it has had and the changes introduced by its revision (eIDAS 2.0 hereinafter), such as the European Digital Identity Wallet (EUDIW hereinafter).

eIDAS 1.0

The advent of the eIDAS regulation, issued on July 23, 2014 and fully effective from July 1, 2016, marked a significant milestone in the European Union's digital transformation

journey (The European Parliament and the Council of the European Union, 2014), with the introduction of a standardized framework for electronic identification and trust services.

This regulation was established with the primary goals of developing the digital single market, promoting cross-border public services, encouraging innovation and competition, and enhancing usability. In fact,

- by ensuring the mutual recognition and interoperability of eIDs and trust services, eIDAS 1.0 sought to eliminate barriers to electronic transactions, thus fostering the growth of the digital economy.
- the regulation facilitated access to public services across the EU, enabling citizens and businesses to use their national eIDs to engage with public administrations in other member states.
- by creating a standardized legal framework, eIDAS 1.0 encouraged competition and innovation within the single market, paving the way for new digital services and business models.
- the regulation aimed to simplify the electronic transactions landscape for individuals and businesses, making digital interactions more user-friendly and accessible.

Despite its significant achievements, the implementation of eIDAS 1.0 encountered several challenges that have threatened its effectiveness in fostering a truly seamless digital single market, particularly regarding the cross-border use of national eIDs, affecting coverage, acceptance, usage, and user friendliness (Bogdan, 2021).

Although eIDAS aimed to standardize electronic identification across the EU, by the time of assessment in 2021, only 19 eID schemes had been notified by 14 Member States: this meant that only 59% of the EU population had access to notified eID schemes, leaving a substantial portion without the means to participate in cross-border electronic transactions. The presence of 7 mobile-based eID schemes highlighted a move towards more accessible digital solutions, yet the overall coverage remained insufficient.

The acceptance of notified eID schemes by Member States was another significant barrier, in fact, while 67% of EU Member States had the capacity to accept notified eID schemes, the actual implementation varied greatly. Among seven key public services identified as critical for cross-border users, only 14% offered eIDAS authentication. This

discrepancy between the potential and actual utilization of eIDAS authentication mechanisms underscored the need for greater harmonization and encouragement for Member States to adopt and implement eIDAS-compliant services.

It is important to note, by the way, that the focus was primarily on the public sector, lacking incentives for the private sector's engagement.

The usage rates of cross-border authentications further illustrated the challenges faced by eIDAS 1.0: the number of successful cross-border authentications per year ranged from 100 to 30,000, a figure that pales in comparison to the millions of authentications occurring at the domestic level annually. The sharp contrast outlined above shows that users are not willing, or not able, to use eIDAS to carry out cross border transactions. Reasons for this could include the aforementioned limited coverage and general lack of acceptance, as well as a general lack of knowledge about eIDAS, or simply a lack of trust in the system.

Finally, the user experience of using eIDAS solutions was far from intuitive: users in fact experienced poor interfaces, redirections during the authentication process and even instances of denial of service. These negative experiences created by the authentication process, deter users from finalising transactions. This does not help to achieve the aim of the regulation to simplify and enhance digital interactions between EU citizens.

These limitations have therefore led to the revision of the regulation: to overcome these challenges and respond to the market and society’s needs today, the still currently proposed improvements include increasing coverage and acceptance, as well as improving the usage rate of cross-border authentications, and providing a uniform and user-friendly experience. The proposed EUDIW in eIDAS 2.0 is expected to address these issues directly and provide a more holistic, inclusive and easy to use digital identity across the EU.

eIDAS 2.0 and the introduction of the EUDIW

The evolution of the digital identity landscape within the European Union has taken a significant step forward in June 2021 with the proposed eIDAS 2.0 regulation (European Commission, 2021). This revision, still ongoing at the time of writing, aims to address the changing digital needs and shortcomings of eIDAS 1.0: while building on the

achievements of its predecessor, it intends to introduce substantial enhancements, that we are going to explore in the following paragraphs.

As anticipated, at the heart of eIDAS 2.0 is the introduction of the EUDIW, a secure and portable digital identity, which will provide natural and legal persons throughout the European Union with a harmonised electronic identification tool to allow authentication and sharing of identity data.

Firstly, by supporting the Self-Sovereign Identity (SSI) model[4], the objective of the inroduction of the EUDIW is to empower EU citizens and businesses with a secure, user-controlled digital identity: in fact, it is expected to give individuals unprecedented control over their personal data and how it is shared, thereby enhancing privacy and data security. At the same time, this wallet aims to significantly reduce the fragmentation of national digital identity solutions and enhance security and convenience for users across the EU: it is being designed to be interoperable across all EU Member States, ensuring that digital IDs and credentials such as driving licenses, health records, and digital travel documents are universally recognized and accepted. Hence, it will reduce the fragmentation of national digital identity solutions, reducing risks and related costs, and facilitating access to goods and services across the EU for citizens and businesses.

The new framework mandates EU Member States to issue digital wallets under notified eID schemes, adhering to common technical standards and obligatory certification: this requirement ensures a uniform, high-assurance level across all Member States, making digital IDs more reliable and widely accepted. By 2024, all EU member states are required to make the Digital Identity Wallet available to any citizen who requests one.

The EUDIW is engineered with robust security measures, featuring strong cryptography and compliance with the EU's GDPR and Cyber Security Act. It enables selective disclosure of attributes by users, allowing them to share only the necessary information for specific transactions.

[4] SSI refers to a new paradigm in identity and access management that improves privacy by ensuring complete control and ownership of personal data by their owners, citizens.

The flexibility and security of the EUDIW are expected to support a broad range of functions and use cases, from online identification and digital signatures to more novel applications that will emerge as the digital ecosystem evolves.

By facilitating digital onboarding and fraud prevention processes, eIDAS 2.0 opens the door to Open Data possibilities, expanding the use of digital IDs beyond the public sector to include banking, healthcare, and other services.
With regards to the industry of interest of this thesis, the banking and financial one, it is likely that a portable European digital identity would be a crucial tool to ensure the financial inclusion and health of individuals and organisations at regional level; in fact, such an identity could potentially allow to easy store and share data beyond personal identity, ranging also from credit history to other factors used in alternative credit scores. From a Fintech company point of view, EUDIW would surely be a great development to leverage the opportunities provided by the Open Banking and Open Finance frameworks.

The table below summarizes the key differences and enhancements from eIDAS 1.0 to eIDAS 2.0.

FEATURE	eIDAS 1.0	eIDAS 2.0
Framework objective	Facilitate secure and seamless digital transactions across the EU.	Expand and refine the digital identity framework to meet evolving digital needs, with a focus on interoperability and user control.
Identification approach	National eID schemes, voluntary for member states, with varying formats and assurance levels.	Standardization of digital identity through the mandatory EUDI Wallet, offering a uniform identification method across the EU.
Assurance levels	Classified into low, substantial, and high, allowing member states to determine the assurance level of their eID schemes.	Mandatory high assurance level for the EUDI Wallet to ensure secure and trustworthy digital interactions.

Private sector inclusion	Member states decide on the inclusion of the private sector and the terms for eID usage.	Mandatory inclusion of the private sector, facilitating broader application and integration of digital IDs in various services (such as Open Banking and Open Finance).
Interoperability	Achieved through voluntary mutual recognition of national eID schemes, leading to fragmented implementation.	Enhanced interoperability and standardization across the EU, ensuring that digital identities are universally accepted and recognized.
User control and data privacy	Limited emphasis on user-controlled identity management and selective data sharing.	Strong focus on user sovereignty over personal data, supporting selective disclosure and data privacy in line with GDPR.
Certification and standardization	eID schemes notified through a peer review process, with diverse standards across member states.	Unified certification process for digital identity schemes, ensuring consistency and high security standards EU-wide.

Table 1: key differences and enhancements from eIDAS 1.0 to eIDAS 2.0

The transition from eIDAS 1.0 to eIDAS 2.0 represents a significant evolution in the EU's approach to digital identity: eIDAS 1.0 created the foundation, eIDAS 2.0 aims to build on that and adapt to the opportunities and challenges of the digital era. With the EUDIW, the EU wants to create a more open, secure and user-friendly digital single market, ensuring that digital identity becomes the engine of innovation which unites Europeans and integrates the continent like never before.

2.5 EUDIW and technical aspects

This subsection explores the technical aspects of the EUDIW, guided by the EC drafted document, that will be referred to as ARF hereinafter, *The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework* (European commission, 2023-a). To guide EU Member States in the creation of digital identities compliant with eIDAS 2.0, this toolbox examines the reference architecture, design considerations, architecture components, and the ecosystem envisioned to facilitate a robust digital identity mechanism.

The EUDIW is designed to operate on mobile phone apps and similar devices, emphasizing time efficiency, reduced administration, enhanced safety, and data protection. One of its core functionalities allows users an almost complete control over which aspects and attributes of their identity to share with third parties, promoting data privacy and control. ‘Almost’ was used because there is a minimal set of attributes that are mandatory for the user to have in the wallet, as shown in *Table 2* below. This user-centric approach is further supported by the EUDIW's adherence to technical standards and certification processes, ensuring a high level of security, referred to as assurance level high, across all user interactions with the system.

Mandatory Attributes	Optional attributes	Possible additional optional attributes
Current family name	Family name at birth	Nationality/Citizenship
Current first names	First names at birth	
Date of birth	Place of birth	Optional attributes used at national level, such as tax number, social security number…
Unique identifier	Current address	
	Gender	

Table 2: Mandatory and optional attributes included in the eIDAS framework (European commission, 2023-a)

The ecosystem of the EUDIW involves multiple stakeholders, as it can be seen in more detail in *Figure 2*, including end users of the wallet (citizens, residents and business in the EU), identity providers (responsible for verifying users' identity and issue digital IDs), service providers (also called *relying parties*, that are the organizations offering digital services to users and "relying" on identity providers for their clients' authentication process), and regulatory bodies (setting standards and governance rules and assessing compliance). Each plays a crucial role in the operationalization and governance of the digital identity framework, ensuring its effectiveness and trustworthiness.

The architecture and reference framework highlights the importance of interoperability with existing national identity systems, with the goal of overcoming the challenges posed by diverse national digital identity schemes: this is achieved through common standards and practices, facilitating the acceptance of digital identities across Member States.

A significant aspect of the EUDIW's implementation is its certification process, which is conducted by accredited public or private bodies appointed by Member States. These Conformity Assessment Bodies (CABs) are responsible for independently assessing wallets to certify that they adhere to EU specifications and standards. This certification

process underscores the EU's commitment to ensuring a secure and reliable digital identity framework.

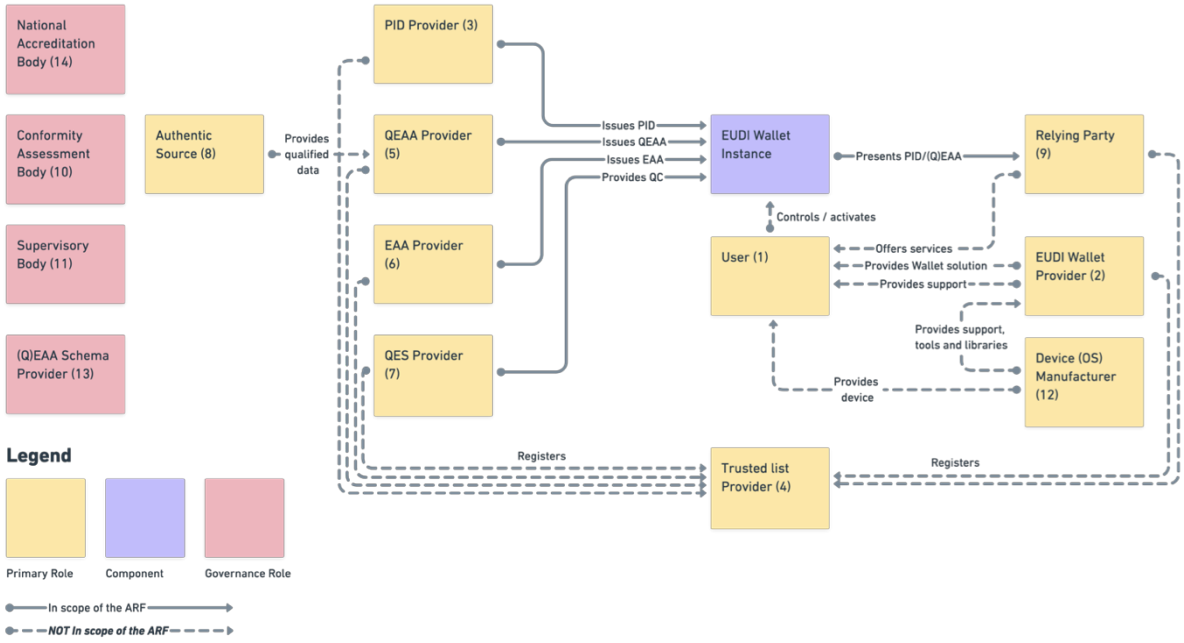

Figure 2: Overview of the EUDI Wallet roles (Source: European commission, 2023-a)

1. End Users of EUDI Wallets

3. Person Identification Data (PID) Providers

5. Qualified Electronic Attestation of Attributes (QEAA) Providers

6. Non-qualified Electronic Attestation of Attributes (EAA) Providers

7. Qualified and non-qualified certificate for electronic signature/seal Providers

In the ARF document also the required levels of assurance for the EDIW can be found: the three defined levels are low, substantial and high. The assurance or trust level reflects how secure the wallet is, and how difficult would it be for a user to steal and use another user's identity. The EDIW must operate at high level of assurance which means that the enrollment and authentication processes must be substantially rigorous in order to provide a higher level of assurance in the claimed identity of a person. This is in line with the

general objective of improving the level of security and reliability of digital identities in the EU.

As we look to the future of electronic identification in the area of Open Banking and Open Finance, we see the EUDIW as a game changer that will revolutionize the digital payments landscape. The evolution from physical wallets to a unified, secure digital identity platform across Europe represents a significant shift towards greater transactional efficiency and better security. The EUDIW captures this paradigm shift by providing a repository where individuals can store and securely share their personal and financial data across borders.

The interoperable EUDIW, accepted by financial institutions across the EU member states to perform SCA, anticipates a new generation of digital payments and is expected to foster significantly higher consumer participation in open banking services under PSD2. By supporting several security factors in user-friendly ways, like biometric information and device attestations, the EUDIW should ensure a much more streamlined authentication process.

Furthermore, the EUDIW, by authenticating the payer during online transactions, could have a significant impact by virtually eliminating unauthorized payment fraud, as evidenced in countries like Sweden and Norway with established digital identity services. This paradigm shift may eventually alleviate the need for banks to develop and maintain their own authentication mechanisms, paving the way for more streamlined banking experiences.

2.6 State of works in Italy with the Italian Digital Identity Wallet

Italy's journey towards issuing its digital identity wallet version (the IT Wallet) exemplifies a national initiative aligning with the broader European Union's digital identity ambitions. The IT Wallet represents Italy's response to providing its citizens with a unified, secure digital identity platform, enhancing access to services and simplifying

digital transactions. This section discusses the progress in developing the IT Wallet, its features and the future it has in Italy’s digital identity ecosystem.

As of early 2024, the development of the IT Wallet has taken major strides. The initial step in this direction was the European Commission publishing the source code, development kits and regulations for national digital wallets on GitHub. This release defines the structure that the national digital wallets have to follow. Therefore, the IT Wallet along with other EU member states’ wallets will have common guidelines to build the general digital identity framework of the European Union. Unlike localized digital identity systems such as Italy's SPID and CIE, the IT Wallet aims to integrate all such systems into a single application, further supported by a €37 million fund allocated for prototype testing in 2022.

The IT Wallet is supposed to work as an application which citizens can use to upload documents like identity cards, driving license, health cards and educational certificates. It will provide citizens with detailed control over their data: users will be able to clearly see which documents and information they want to make available and which they will keep back in non-default, hidden sections.
The IT Wallet will facilitate proximity and remote checks and authentications and will offer different types of authentication like PIN codes, passwords, biometric systems and one-time passwords (OTP), aligning with the European Commission advice of adopting multiple systems depending on the sensitivity of the data and specific circumstances, ensuring a balance between convenience and security.

Italy is targeting to launch the IT Wallet by the summer of 2024 and eventually plug it into the obligatory EUDIW framework by 2026. The future of digital identity in Italy depends on how the users react to the IT Wallet: will it be embraced by them in large numbers, what will be the adoption rate and what will be its effect on the existing digital identity ecosystem?
The integration of IT Wallet into the AppIO, the government's digital services platform, marks a strategic move to streamline access and enhance user experience and aims to familiarize Italian citizens with the digital wallet's functionalities.

Overall, the IT Wallet initiative reflects Italy's proactive stance on digital transformation, aligning with EU standards while addressing country-specific requirements. As this initiative unfolds, it holds the promise of reshaping Italy's digital identity landscape, offering a more cohesive, secure, and user-centric approach to digital identification and service access.

CHAPTER 3: LITERATURE REVIEW AND RESEARCH QUESTION

3.1 Literature Review

In the European Union, there is a strong political motivation to upgrade the digital identity frameworks, as visible with the revision of the eIDAS regulation and the proposal of the EUDIW. Interoperability and security of online identities is something that the community working on digital identity and authentication has been struggling with for a long time. Academic debate has largely explored the design, challenges, and potential of digital identity wallets, establishing a favourable ground for further innovation in this critical sector.

This literature review aims to synthesize these discussions, highlighting the need for a deeper examination of how these systems align with various socio-economic contexts: in fact, it identifies gaps in existing research, particularly the lack of a comprehensive model that correlates digital identity systems with the socio-economic structures of the different countries in which they are implemented successfully. This underscores the necessity for an analysis that not only integrates the best features of existing solutions but also adapts them to meet the specific needs of diverse national contexts, and that would be invaluable for experts aiming to develop or refine digital identity wallets that are both effective and contextually appropriate within national frameworks.

The trajectory of digital identity systems has been shaped by evolving regulatory frameworks and technological advancements.
Dib et al. (2020) provide in their work a comprehensive analysis that outlines the evolution from centralized to federated and then to decentralized models, highlighting the increasing need for scalability, interoperability, privacy, security, and regulatory compliance in identity systems. The challenges identified, including the scalability of

blockchain platforms and the necessity for interoperable frameworks that can operate across jurisdictions while protecting user privacy and ensuring security, mirror the issues currently being addressed in the development of digital identity frameworks within the EU.

Czerny et al. (2023) discuss the transition from traditional cross-border eID systems to modern wallet-based systems within the EU, stressing the need for constant adaptation that takes into account existing solutions, while taking advantage of new technologies for greater security and control of users. Similarly, Schwalm (2023) examines the implications of the eIDAS 2.0 framework, which introduces decentralized technologies and the EUDIW to overcome the limitations of the original eIDAS regulation.

Despite the technological progress, there are still many hurdles to overcome before digital identity wallets can be widely used and function properly: inconsistent data specifications, a lack of interoperability and inadequate governance models are some of the major challenges that prevent public and private stakeholders from working together effectively, as claimed by Lukkien et al. (2023). This is also confirmed by Schwalm (2023), who illustrates some technical and regulatory barriers to the implementation of the updated eIDAS framework in Europe.

A critical aspect of digital identity wallets is their user experience (UX), which could have a major impact on their adoption and effectiveness. Krauß et al. (2023) explore user-centric design principles for digital wallets, developing scenarios that integrate user-friendly features for everyday use. Complementing this view, Sellung and Kubach (2023) provide a state-of-the-art review of the UX of digital identity wallets and suggest improvements to make the use of such platforms easier for citizens while maintaining security and privacy. Intuitive usability and user empowerment in terms of control over their personal data are crucial for acceptance and trust in digital identity wallets, they argue.

The technology behind digital identity wallets is a key aspect to consider because it has a direct impact on their usability and security. Abraham et al. (2021) focus on the use of mobile-phone based identity wallets that reach high levels of assurance, essential for

sensitive applications like eGovernment services. They propose a wallet architecture that incorporates robust security measures such as hardware-based secure elements and multi-factor authentication, ensuring a high degree of user trust and data protection.

3.2 Research Question

To the best of my knowledge, while the literature extensively covers various aspects of digital identity wallets, from regulatory challenges and technical implementations to UX design and security considerations, it lacks a comprehensive scheme that correlates specific socio-economic structures of countries with their most effective digital identity system models. Current discussions fail to systematically align the characteristics of a country's socio-economic environment with a digital identity framework that best suits its unique needs. This gap presents an opportunity to create a sort of contingency theory for digital identity wallets at the country level. In a manner analogous to how contingency theory suggests that the optimal management, organizational structure, and decision-making processes within a corporation are contingent on specific internal and external factors, this research aims to propose that the most effective digital identity systems are similarly dependent on the socio-economic and institutional contexts of their respective countries, requiring adaptable strategies that are tailored to meet these unique conditions.

My work aims to fill the identified gap by analyzing a selection of successful federated digital identity wallets across several countries, examining how these systems effectively establish trust, control credential sharing, and ensure widespread accessibility. This analysis will not only identify the critical features that contribute to the success of these systems but will also generalize the findings to suggest ideal digital identity models for countries with similar socio-economic characteristics.
For example, by studying India's Aadhaar system, which has proven successful in a developing country context, I will extract the features that have underpinned its success in establishing trust, managing credential sharing, and ensuring accessibility. These features will then be abstracted to suggest a model that could likely succeed in similar developing country contexts. Analgously, analyses of other countries' positive

experiences will provide distinct abstractions based on their respective socio-economic environments, which can guide other states in developing or refining their digital identity solutions.

This approach will offer practical guidance for policymakers and designers tasked with developing secure, trustworthy, and inclusive digital identity infrastructures in different socio-economic settings.

In particular, the research question that will guide my analysis is the following:

How do existing digital identity wallet arrangements align with institutional structures and digital strategies at the country level, and how can these systems balance security, privacy, and user experience within their specific socio-economic contexts?

This question seeks to investigate the alignment between digital identity systems and the broader institutional and strategic frameworks within which they operate and how these systems succeed in their specific environments by examining their key features and how these features meet the particular needs of their socio-economic context.

CHAPTER 4: METHODOLOGY

This chapter outlines the empirical methodology employed in this research to investigate how digital identity systems align with the socio-economic structures and institutional strategies of different countries. Given the complexity and diversity of digital identity systems worldwide, this analysis focuses on a comparative study of selected cases that exemplify distinct approaches to digital identity management.

The primary challenge of this analysis is to abstract the key features of successful digital identity systems and generalize them into a model that can guide their development in similar socio-economic contexts.

4.1 Rationale

Research objective

As previously stated, the primary objective of this research is to develop a contingency theory that matches specific digital identity systems with the socio-economic structures of different countries. By analyzing successful digital identity systems across varied national contexts, this study aims to abstract key features that contribute to their success in terms of security, privacy, and user convenience. These insights will be used to suggest digital identity models that could be effectively implemented in other countries with similar socio-economic characteristics. This systematic approach seeks to provide a framework that not only enhances understanding of why certain digital identity systems succeed but also guides the development of new systems, particularly in contexts that are considering the adoption or enhancement of their digital identity infrastructures.

Choice of empirical context

The empirical context for this investigation encompasses four case studies, each exemplifying distinct approaches to digital identity management influenced by their specific socio-economic and institutional environments:

- *Estonia's eID*: this government-led initiative offers insights into a state-driven digital governance model, highlighting the integration of digital identities with public services and civic engagement.
- *Sweden's BankID*: a private sector-driven model that demonstrates the impact of collaborative efforts between banks and technology providers on widespread service adoption and trust.
- *India's Aadhaar*: the world's largest biometric ID system, emphasizing an inclusive approach that addresses the needs of a diverse and populous developing country.
- *Singapore's SingPass*: a technology-centric strategy that leverages advanced digital technologies to enhance efficiency and accessibility in public and private sector interactions.

These case studies were selected for their diversity in approach and geographical representation, providing a wide range of insights into how different socio-economic factors influence the effectiveness and design of digital identity systems. Each system offers unique perspectives on handling the challenges associated with digital identity management, making them ideal for a comparative analysis aimed at deriving generalizable principles that can inform the development of digital identity solutions in other socio-economic contexts.

4.2 Method

Data collection

The data for this study were primarily collected from secondary sources, including academic articles, government reports, technology white papers, and case studies. Secondary data were chosen due to the extensive documentation available on each digital

identity system, which allows for a comprehensive analysis without the logistical and financial constraints of primary data collection.

Advantages of secondary data

Utilizing secondary data provides several advantages.

First of all, access to pre-existing data sets enables a more efficient analysis process, as the information has already been collected and often validated. In terms of scope, this is particularly useful in synthesizing broad trends and long-term developments in digital identity systems that would be difficult and time-consuming to gather firsthand.

Ultimately, published data from reliable sources ensure that the information is comparable across different contexts, which is essential for this study's cross-case analysis. In fact, data from reliable sources are generally collected and presented in a consistent manner and this uniformity is crucial when comparing data across different cases or contexts, as in this thesis, where I am examining digital identity systems from various countries, each with its own unique set of cultural, technological, and regulatory frameworks. Reliable secondary data provide a standardized format that makes it possible to directly compare these diverse systems.

4.3 Analysis

Data processing

Data were systematically organized into categories corresponding to the dimensions of trust establishment, credential sharing control, and accessibility assurance, so as to facilitate a structured comparison across the different systems.

Analytical approach

The analytical framework of this study is designed to systematically examine and compare selected digital identity systems through a structured thematic analysis, which is ideal for identifying patterns, themes, and variations across the case studies and for understanding how digital identity management works within the various socio-economic and institutional contexts.

For each case study, the analysis begins with a contextualization phase, addressing a standardized set of questions aimed at capturing the socio-economic situation of the country and the fundamental characteristics and operational aspects of its digital identity system. These questions include:

1. Providing an overview of the country being analyzed from a socio-economic perspective, focusing on factors that influence digital infrastructure and policy, such as economic development, digital literacy, and societal norms.
2. Identifying the type of digital identity solution (e.g., web-based, mobile-app-centric…) to understand the accessibility and user interface of the system.
3. Determining whether the identity wallet is developed and managed by public sector entities, private sector organizations, or a collaboration between both, to get insights into the governance structure and potential biases in the system's design and functionality.
4. Examining the underlying trust model used for the digital identity system, such as reliance on centralized databases, decentralized networks, or blockchain technology.
5. Additional questions will further explore regulatory compliance, interoperability with other systems, user experience considerations, and the technological infrastructure supporting each system.

Following the contextualization, the study will continue with a thematic analysis where convergent and divergent themes across the case studies are identified. This stage will focus on the three core dimensions previously outlined:

- Trust establishment: we are going to analyze how each system builds and maintains user and institutional trust, including mechanisms for ensuring authenticity, integrity, and confidentiality of identity data.
- Credential sharing control: we will then examine how each system manages and controls the sharing of credentials, analyzing user consent mechanisms, data minimization practices, and the ability to control which parts of an individual's identity are shared and with whom.
- Accessibility assurance: finally we will continue by assessing how each system ensures that its services are accessible to a broad user base, including

considerations for digital literacy, technological barriers, and support for multiple languages and formats.

This thematic analysis will allow for the extraction of key features and challenges inherent in each system, offering insights into how these features correlate with the specific socio-economic environments. The findings will aid in generalizing these features to suggest models for other countries with similar socio-economic characteristics, contributing to the development of a synthesized framework that aligns with eIDAS 2.0 standards and addresses the gaps identified in current implementations. The comparative nature of this analysis will also guide policymakers and designers in developing effective digital identity solutions tailored to diverse socio-economic settings.

CHAPTER 5: ANALYSIS AND THEORY FORMULATION

5.1 Comparative analysis of case studies

5.1.1 Estonia's eID

5.1.1.1 Socio-economic context

Political and economic prosperity and stability

As a democratic parliamentary republic with active memberships in the EU, NATO, and the OECD, Estonia enjoys a high level of political stability and economic prosperity, which is beneficial for the support and development of advanced digital infrastructures.

Estonia's economic environment, characterized by a robust financial sector and sound fiscal policy, has built over the years a reputation for resilience and innovation, particularly in digital technologies: this stable economic framework is indispensable to sustain continuous investment in technology and supporting developed governance initiatives like Estonia's eID, that we will deepen in the next section.

The ability that the nation has shown in navigating economic shocks, such as the global financial crisis and the recent pandemic, without destabilizing its digital governance agenda, is an evidence of the strength and foresight of its economic policies.

Digital governance and innovation leadership

Estonia stands as a global leader in digital governance and innovation, pioneering numerous digital-first initiatives that have become benchmarks worldwide. The country's proactive approach to digitalization is deeply embedded within its governance structures, supported by strong institutional frameworks and a strategic vision that emphasizes efficiency, transparency, and citizen engagement.

This leadership in digital innovation is facilitated by an overarching governmental support system and a clear policy direction that prioritizes digital integration in all aspects of public administration: such an environment not only encourages the growth of digital technologies but also ensures that these innovations are effectively integrated across government and public services, enhancing their functionality and reach.

Human capital and digital literacy

One of the reasons for Estonia's digital success is surely its highly educated and digitally literate population; in fact, the country can boast of one of the highest literacy rates in the world, supported by a comprehensive educational system that integrates digital skills training from early schooling. This focus on education is reflected in the Human Capital Index[5], where Estonia scores a remarkably high 78%, indicating that a child born today in Estonia will achieve 78% of their potential productivity with complete education and full health by the age of 18.

Estonia's focus and investment on digital literacy is evident through its national curricula and public initiatives that aim to equip citizens with the necessary skills to adopt, navigate and exploit digital platforms effectively. This widespread digital proficiency is crucial for the adoption and effective utilization of systems like the eID, ensuring that such technologies are accessible and beneficial to the entire population.

Technological integration and public policy

The government of Estonia has placed great strategic importance on digital transformation, which can be seen in both its public and private sector initiatives. The various plans for recovery and resilience already developed in this country emphasize the importance of enhancing service delivery through technology, aiming for a seamless integration of digital solutions into everyday life. Regarding the thesis topic, this strategic approach promotes the broad acceptance and practical use of digital identity and ensures that these systems are robust, secure, and user-friendly.

[5] The Human Capital Index (HCI) "measures the amount of human capital that a child born in 2018 can expect to attain by age 18 in view of the risks of poor education and poor health that prevail in the country in which she was born." (World Bank, 2019)

Estonia's policies demonstrate a clear understanding of the transformative power of digital technologies, as seen in the government's commitment to maintaining a cutting-edge digital infrastructure, and they are designed not only to supports the current needs of Estonia's digital governance but also to anticipate future developments, ensuring that the nation remains always at the forefront of digital innovation.

Estonia's Digital Agenda 2030: envisioning a fully digitized society

As mentioned so far, Estonia has long stood on the front lines of digital innovation, leveraging technology either to transform public services, enhance connectivity, or maintaining a secure cyberspace. The Estonia *Digital Agenda 2030*, promoted by the Ministry of Economic Affairs and Communications, builds on this legacy, aiming to elevate Estonia into a leader of digital empowerment by 2030. This strategic plan, in alignment with the national long-term strategy *Estonia 2035*, outlines a future where digital solutions enhance the quality of life and drive economic development through a robust, secure, and inclusive digital society.

The primary goal of the Digital Agenda 2030 is to offer all citizens a high-quality, accessible, and seamless digital experience, thereby enhancing their daily lives, economic activities, and security. The agenda has been designed for Estonia to acquire digital *vägi* (power), in order to continue building a society where advanced digital solutions lead to superior living standards and economic efficiency.

While Estonia is celebrated for its digital government initiatives, challenges such as enhancing user experience, achieving widespread high-speed internet access, and continuously updating cybersecurity measures need addressing. Indeed, the three key areas of focus of the agenda are digital government, connectivity and cybersecurity.

First, the agenda prioritizes the evolution of digital government services to ensure they are proactive, operate in the background, and are centered around user needs. This involves as well refining the eID system to make it more user-friendly and versatile, adapting to technological changes and increasing the integration of biometrics and other modern authentication methods.

The ongoing development of the state portal and the enhancement of digital identity tools reflect efforts to make governmental digital platforms more sustainable and accessible: this includes improving the interoperability of data exchange systems both domestically

and internationally. Estonia actively engages in strategic international collaborations to enhance the interoperability of its digital solutions with European standards, allowing for efficient cross-border digital operations; in fact, it actively participates in policy-making within the EU and other international bodies to share knowledge and promote Estonian digital innovations globally.

As regards connectivity, to support the widespread adoption of digital services, Estonia is committed to expanding the availability of fast, reliable, and affordable digital connections nationwide. This infrastructure is vital for the universal accessibility of the government's digital services.

Lastly, with the digital landscape constantly evolving, enhancing cyber defenses is essential to protect national infrastructure and ensure the trustworthiness of digital interactions: continuous improvements in cybersecurity measures are necessary to address emerging risks and maintain Estonia's reputation as a secure digital nation.

The Digital Agenda 2030 is implemented through detailed annual action plans that specify activities, measures, and responsibilities and this dynamic approach allows for adaptability to new developments and challenges. Moreover, the agenda emphasizes public consultation and the importance of collaboration with private sectors and international partners to foster a participatory development process and integrate best practices from around the world.

All things considered, the Estonia Digital Agenda 2030 aims ambitiously to consolidate Estonia's role as a global digital leader: by leveraging cutting-edge digital technologies, Estonia seeks to enhance the operational efficiency of its public services and to improve economic opportunities and social inclusion. Through this comprehensive digital transformation, Estonia envisions creating a society that is not only connected and secure but also innovative and forward-thinking.

Influence of socio-economic factors on Estonia's digital identity strategies

Estonia's socio-economic context has significantly influenced its digital identity strategies, with political stability, economic strategies, educational policies, and a commitment to digital innovation playing pivotal roles: these factors have collectively enabled the development of a digital identity framework that is advanced, secure and deeply integrated within the nation's social and economic fabric. Through the Digital

Agenda 2030, Estonia continues to refine and expand its digital identity systems, ensuring they remain effective and relevant, thus setting a global standard for digital governance and citizen engagement.

5.1.1.2 Estonia's eID system overview

Estonia is well known worldwide for its advanced digital government services, and at the heart of those lies its national digital identity scheme, the Estonia eID. Launched in 2002, the eID infrastructure is a cornerstone of the nation's e-governance infrastructure, enabling secure and convenient transactions between the state, citizens and private sector entities. As one of the most widely used foundational ID systems in the world, it allows e-citizens to authenticate themselves to most services and is used in a wide variety of applications from electronic voting to tax declaration, from e-health services to banking. It plays a key role in making digital identity an integral part of people's daily lives.

Types of digital identity solutions

Estonia's eID system offers a multifaceted approach to digital identity, incorporating both physical and digital methods to ensure widespread accessibility and ease of use, as listed below:

1. *ID-card*: Estonia issues a national ID card equipped with an electronic chip that serves as a legal travel document within the EU and a national identity card outside of it. The embedded chip contains encrypted digital keys and certificates that enable digital authentication and electronic signatures. Every Estonian citizen and resident from the age of 15 is required to have this card.
2. *Mobile ID*: To enhance accessibility and user convenience, aligning with the global trend towards mobile-centric digital solutions, Estonia introduced the Mobile ID program in 2007. This system integrates digital identity functionalities into a SIM card, which can be used in mobile phones, so that users can perform secure transactions and access e-services directly through their mobile device without the need for a physical card reader.
3. *Smart-ID app*: This widely used app does not require a SIM card and can operate on any smart device, including tablets. It is particularly favored for its

convenience in performing secure transactions and signing documents digitally. Importantly, Smart-ID acts as a simple, easy-to-use alternative to traditional bank code cards, allowing users to log into financial sector e-services and confirm transactions and agreements, thereby playing a crucial role in the context of Open Banking and Open Finance.

4. *e-Residency*: Launched in 2014, Estonia's e-Residency program offers a transnational digital identity to global citizens, enabling access to Estonian public e-services and the EU business environment. E-residents can set up and manage a location-independent EU company online, apply for a business bank account, conduct secure e-banking, access international payment service providers, digitally sign documents, and declare Estonian taxes online. This program is particularly beneficial for entrepreneurs looking to operate globally without physical constraints.

Accessibility and user interface

Estonia's eID system, with its diverse solutions offer, is designed to be inclusive and user-friendly, accommodating a broad demographic: as just seen, the physical smart cards requiring card readers are complemented by mobile solutions allowing users to access services directly from their devices and this multi-modal approach ensures that all citizens can engage with e-services in a manner that suits their technological preferences and capabilities.

The interfaces for the Smart-ID app are designed with simplicity and user experience in mind: the application is simple and fast to use, with clear prompts, step-by-step authentication processes, and minimalistic design; it is also designed to be used in different types of devices.

For example, if a user having a Smart-ID account wants to apply for a loan, the bank could conveniently use Smart-ID to verify the identity. As shown in *Figure 3*, the bank would allow the user to login using Smart-ID by requesting country and personal national identity number, then a code (PIN2) would be displayed to be compared to the one shown in the Smart-ID mobile app. If they match the user can confirm his identity by inserting his personal PIN code (PIN1).

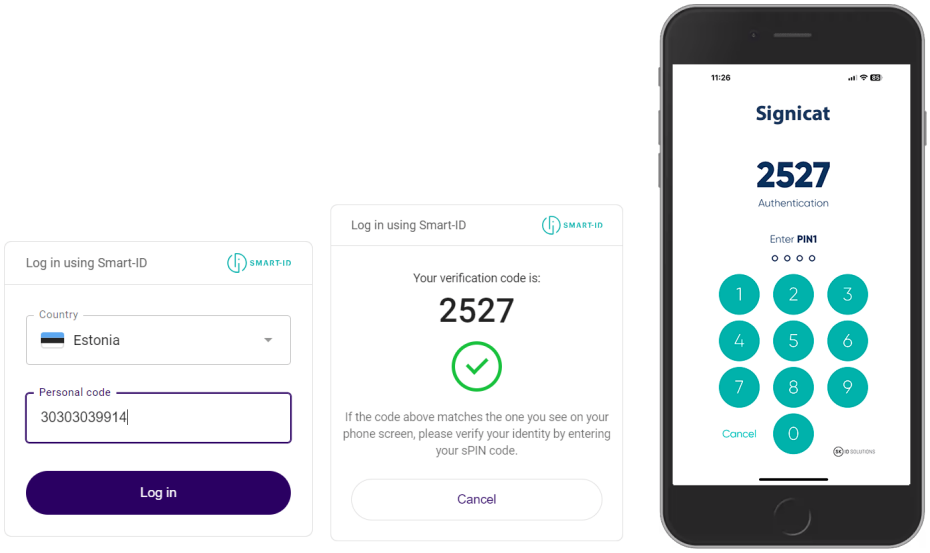

Figure 3: Screen example of Smart-ID app usage. The first two interfaces belong to a bank mobile app: the first one is the login interface that utilizes Smart-ID identification, and the second one displays a code to the user. Then the user moves to the Smart-ID app (third interface) and sees a code displayed: if it matches the one shown in the bank app he inserts his personal PIN confirming the identification.

Use case can be found at: https://developer.signicat.com/identity-methods/smart-id/about-smart-id.html#use-case-examples

Additionally, Estonia's eID system is seamlessly integrated with a myriad of services, enabled by the X-Road data exchange platform (we will delve into it later in the section) that underlies the country's digital infrastructure. This integration ensures that users can access various services through a single digital identity, simplifying the user experience and enhancing the usability of digital identity across different sectors.

Governance and management of Estonia's eID system

Estonia's eID system is the result of an intricate combination of governance and management primarily by public sector entities, with strategic involvement of the private sector. This governance structure plays a critical role in the system's design, functionality, and overall success in integrating digital identity across governmental and private services.

The primary responsibility for developing and managing the Estonia eID system lies within the public sector: key public authorities such as the Police and Border Guard Board (PBGB) and the Estonian Information System Authority (RIA) play central roles. In particular, the PBGB is responsible for issuing digital identity documents, overseeing their production, and managing the legal and procedural frameworks that govern identity verification and document security; meanwhile, the RIA handles the technological infrastructure, ensuring the security, reliability, and functionality of the digital identity services.

This centralized public sector management ensures that the eID system aligns with national security standards and public policy objectives, which include widespread digital accessibility, protection of personal data, and the promotion of e-governance.

Although the public sector leads the development and management of the eID system, Estonia also leverages public-private partnerships to enhance technological and operational capacities. These partnerships primarily involve technology and security providers, telecommunications and software development companies.

Private companies play crucial roles for example in the physical production of ID cards and the provision of technological solutions such as the security features of digital IDs and mobile solutions. For example, the French company IDEMIA has been involved since 2017 in manufacturing newer generations of ID cards, integrating advanced security technologies.

In the Mobile ID segment, Estonian major telecom operators provide essential infrastructure that supports the functionality of mobile digital identities. These companies deploy special SIM cards that facilitate secure mobile authentication and digital signing processes, broadening the accessibility and usability of digital identities.

Private sector contributions are also significant when it comes to software development for eID applications: to this purpose, companies collaborate with public sector agencies to develop and maintain essential applications like *DigiDoc4*, which is used for document signing and management.

The involvement of both public and private sectors in managing Estonia's eID system brings several advantages, including innovation, efficiency, and enhanced service delivery.

However, this collaboration also necessitates robust oversight mechanisms to prevent potential biases in system design and functionality: the primary concern is ensuring that private sector interests do not overshadow public good, particularly in terms of data security and user privacy. To mitigate such risks, the Estonian government ensures that legislative and regulatory frameworks like the eIDAS regulation and GDPR are strictly followed, and oversight bodies like the Data Protection Inspectorate provide an additional layer of scrutiny, ensuring that all stakeholders adhere to the highest standards of data protection and security.

Trust model of Estonia's eID system

Estonia's eID system is an example of advanced digital identity management, employing a comprehensive trust model that integrates centralized databases, decentralized networks, and blockchain technology to ensure security, reliability, and trustworthiness. This recurring multi-faceted approach is key in maintaining the integrity and functionality of one of the world's most integrated and successful digital identity systems.

At the heart of Estonia's eID system is its reliance on centralized databases to store critical personal data and digital certificates associated with electronic IDs. These databases are managed by trusted government agencies, ensuring that the data is secure and regulated under strict data protection laws and standards. The centralized nature of these databases allows for efficient management and quick access to information, which is essential for the functionality of numerous e-services across public and private sectors.

The PBGB plays a significant role in this aspect, overseeing the issuance and management of digital identity documents: centralized databases enable the PBGB to perform real-time verification of identities and manage the lifecycle of digital credentials effectively.

In addition to this, Estonia enhances the robustness of its eID system through the use of X-Road, a free, open-source and decentralized data exchange layer that facilitates secure communication between various public and private sector information systems. X-Road allows for the interoperable use of e-services, ensuring that data can be securely accessed and shared across different platforms without the need for central mediation. This decentralized approach reduces the risk of data silos and enhances the resilience of the system against cyber-attacks.

X-Road's architecture is built on a distributed trust model, where each participant operates its security server (see *Figure 4*). These servers serve as the gateway to X-Road, facilitating secure service transactions between Information Systems: in fact they are responsible for encrypting and decrypting messages, managing digital signatures, and ensuring the integrity and confidentiality of data as it travels across the network.

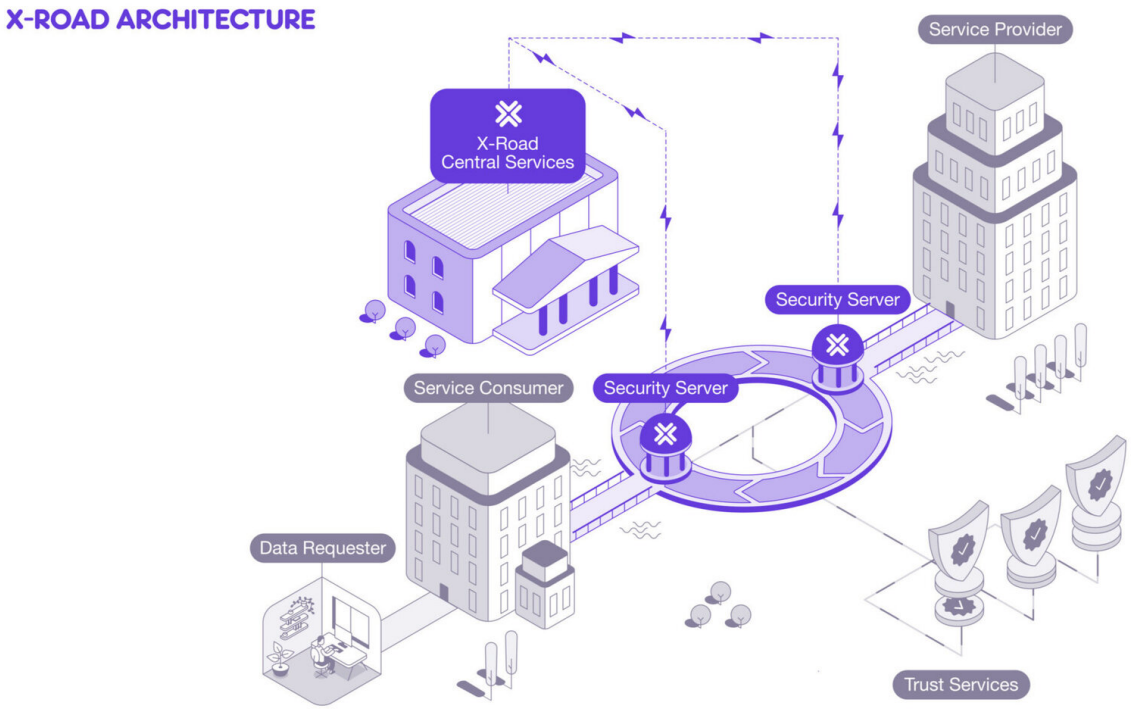

Figure 4: X-Road architecture.

Available at: https://x-road.global/architecture

Estonia eID's trust model incorporates as well blockchain technology through the employment of the Keyless Signature Infrastructure (KSI) Blockchain. This technology is used to ensure the integrity of data logged within the eID system and to prevent tampering and unauthorized alterations of digital records, by providing an immutable cryptographic proof of any data changes.

The use of blockchain enhances the overall trustworthiness of the digital identity system by providing a transparent and verifiable method of tracking data changes over time: this is particularly important in legal and financial contexts.
Moreover, critical systems are designed for high availability with redundancies and failovers to ensure continuous service delivery: data embassies, for instance, like the one they built in Luxembourg, host backup servers in foreign countries to protect against major incidents or disasters.
Finally, comprehensive security measures including encryption and multi-factor authentication protect the system against unauthorized access and data breaches.

The integration of centralized databases, decentralized networks, and blockchain technology provides a layered security approach that is central to the trust model of Estonia’s eID system. This model ensures that while data is centrally managed for efficiency, it is also protected through decentralized and cryptographic measures to enhance security and trust.
The trust model thus defined addresses several critical aspects: in terms of security it protects data against unauthorized access and cyber threats; as regards privacy it ensures that personal information is handled according to strict data protection standards; for what concerns interoperability, it facilitates the seamless exchange of information across various services and platforms; and from a transparency and accountability stand point, it provides mechanisms for auditing and tracking data transactions to maintain public trust.

Regulatory compliance
Estonia's eID system is closely aligned with both national and European Union regulations, ensuring compliance with high standards for digital identity management. Among the key regulatory frameworks we can find the eIDAS regulation and GDPR at the union level and some other local legislation.
Estonia's eID system conforms to the previously analysed EU's eIDAS regulation: the system's notification under eIDAS with an assurance level "high" entails its compliance with the strictest security and operational benchmarks set by the EU.

Compliance with GDPR is critical for protecting personal data and privacy, and in particular the eID system incorporates GDPR principles by ensuring data minimization, secure data processing, and providing users with control over their personal information. By adhering to regulations such as eIDAS and GDPR, Estonia's eID system has been designed to be interoperable at the international level, particularly within the EU, allowing Estonian eID holders to use their digital identities across EU member states for a variety of services.
Finally, the system adheres to Estonian laws such as the Electronic Identification and Trust Services for Electronic Transactions Act, which governs the use of electronic identification and trust services within Estonia and ensures that all processes involving digital identities meet national security and privacy standards.

Having explored the sophisticated digital identity framework in Estonia, we now turn our attention to another noteworthy example in Europe, Sweden's BankID system, a model of digital identity that highlights a different approach primarily driven by the banking sector.

5.1.2 Sweden’s BankID

5.1.2.1 Socio-economic context

Political and economic stability
Sweden's socio-economic environment is defined by long standing political stability, robust economic management and a competitive and open market system, which is highly integrated with global markets.
Sweden provides a participatory and representative type of governance as a parliamentary democracy with a constitutional monarchy: this political framework ensures that the governance system is responsive and adaptable, enabling a favourable environment for the implementation of innovative digital initiatives.

Economic management in Sweden is characterised by prudent fiscal policies and a strong welfare state, that both contribute to comprehensive social services and a generally high standard of living, and support a stable economic environment by reducing inequality and encouraging inclusive growth, which are vital for preserving social cohesion and economic stability.

The strategic focus of the Swedish government on technological innovation and digital governance further strengthens the country's economy. By actively promoting the digitalization of public services, Sweden enhances the efficiency and accessibility of government interactions for its citizens and businesses.

Furthermore, Sweden's strategy of integrating underprivileged groups and emphasising digital literacy ensures that all segments of society can participate in and benefit from the digital economy, thereby enhancing overall productivity and economic stability.

Digital governance and infrastructure

Sweden has always been a frontrunner in digital governance, thanks to its advanced digital infrastructure that ensures comprehensive connectivity across both urban and rural areas. High internet penetration rates and ongoing investments in broadband connectivity facilitate the seamless operation and universal access of digital services. The government actively promotes the digitalization of public services, making them more accessible and efficient, which is, among others, central to the success of digital identity systems.

These efforts are supported by robust cybersecurity measures, ensuring the safety and reliability of digital interactions and data integrity.

Integration of disadvantaged groups, human capital and digital literacy

As previously mentioned, Sweden's socio-economic policies particularly emphasize inclusivity, focusing on the integration of disadvantaged groups, including immigrants and low-income families, into the digital society: the Swedish approach to digitalization is designed to be aimed at everyone, supporting efforts to bridge the digital divide and ensure that all segments of society can benefit from digital advancements.

In addition to inclusiveness, the Swedish government invests heavily in human capital, which is evident through its robust public education system, and stresses digital literacy as a fundamental component of citizens' curriculum: Swedish children receive early

education in digital skills, preparing them for a highly digitalized environment. The widespread digital literacy ensures that citizens are well-prepared to engage with digital platforms securely and effectively and that they are able to adapt to new technologies, and, in the context of digital identities, it facilitates their adoption.

Technological integration and public policy

Sweden exemplifies a nation where technological integration is deeply embedded in both policies and practice, creating an active ecosystem that drives innovation across its industrial landscape. The Swedish government actively fosters this integration through strategic public policies aimed at enhancing the nation's digital infrastructure and encouraging the adoption of advanced technologies in all sectors of the economy. Initiatives like IndTech, regarding co-creation and sharing of knowledge about digital solutions and Sustainable Production, a platform where Swedish technology providers industry stakeholders collaborate to achieve sustainable environmental goals, both in the manufacturing sector, underscore Sweden's commitment to merging information technologies with operational technologies, promoting efficiency and adaptability in manufacturing.

These efforts are supported by a well-established tradition of collaboration between the public sector and private enterprises, ensuring that technological advancements are broadly accessible and effectively implemented.

Influence of socio-economic factors on Sweden's digital identity strategies

The socio-economic factors in Sweden, including political and economic stability, inclusive digital policies, and a strong emphasis on technological innovation, have significantly influenced the country's approach to digital identity strategies. These factors have enabled Sweden to implement a digital identity system that is secure, inclusive, and integrated with national policy goals, setting a benchmark for digital identity systems worldwide.

In the following section we are going to explore the Sweden's electronic identification system: BankID.

5.1.2.2 Sweden's BankID system overview

Origins, expansion and impact

Sweden's BankID was initiated in the early 2000s as a collaborative effort primarily driven by major Swedish banks, and then the system was launched in 2003, marking a significant step in the country's digital evolution. It was developed with the intent to provide a secure and uniform method for digital identification and electronic signatures across various services.

The development of BankID represents an example of successful collaboration among financial sector institutions: major Swedish banks such as Swedbank, SEB, and Handelsbanken played pivotal roles, recognizing the need for a unified digital identity solution that could serve not only banking but also a wide range of other public and private services. This collaborative effort was underpinned by the recognition that a shared digital identity system could enhance efficiency, reduce costs, and improve customer experience across sectors.

The establishment of BankID was significantly supported by public-private partnerships, illustrating a model where governmental encouragement and regulatory frameworks facilitated private sector innovation and implementation. The Swedish government provided a regulatory environment that ensured the security and reliability of digital identities, which in turn encouraged widespread adoption across various sectors, including healthcare, government services, and the private sector.

The success of BankID is also attributed to Sweden's advanced digital infrastructure: indeed, high internet penetration, widespread use of digital technology, and robust cybersecurity measures provided the necessary foundation for implementing a national digital ID system. Technological providers and telecom companies were integral to this process, offering the necessary hardware and software solutions that ensured the reliability and scalability of BankID.

Over the years, BankID has evolved to accommodate the growing needs of digital services and the increasing demands for secure electronic identification and signatures. It has also expanded to include mobile solutions, reflecting the global trend towards mobile-centric digital solutions: the mobile version of BankID has become particularly popular

due to its convenience and ease of use, allowing users to perform secure transactions and access services on-the-go.

BankID has profoundly impacted Swedish society by providing a secure and efficient means of accessing a wide array of digital services: it has become a critical component in the digitalization of the Swedish public and private sectors, facilitating everything from online banking to tax filings and interactions with healthcare providers. The system's success is reflected in its high adoption rates, with a significant proportion of the Swedish population actively using BankID for daily digital interactions.

Type of digital identity solution

Sweden's BankID is a versatile digital identity solution that is available both from web-based and mobile-app-centric platforms, ensuring broad accessibility and user-friendly interfaces across various devices.

As a foundational component of Sweden's digital infrastructure, BankID supports diverse applications, from online banking to government services.

The system includes several operational modes: Mobile BankID, where credentials are securely stored on mobile devices, providing users with the convenience and accessibility to perform digital verifications directly from their smartphones; BankID on File, which involves credentials downloaded and stored on personal computers for those preferring desktop access; and BankID on Card, featuring a smart card application for users desiring physical tokens. This multifaceted approach not only takes into account different user preferences but also enhances the security layers of the digital identity by adapting to various usage contexts.

The integration of BankID across mobile and web platforms highlights its role in facilitating seamless and secure user interactions, making it a determining element in the digitization of personal and commercial transactions in Sweden.

Governance structure of Sweden's BankID

Sweden's BankID system exemplifies a collaborative governance structure, developed and managed through a partnership between private sector banks and public sector oversight. The system was originally developed by a consortium of major Swedish banks, highlighting its strong roots in the private sector. These banks, including Danske Bank

(the only Danish bank), Handelsbanken, Länsförsäkringar Bank, SEB, Skandiabanken, and Swedbank, collectively oversee the operational and strategic directions of BankID through Finansiell ID-Teknik BID AB, the entity responsible for BankID's development and maintenance. This private sector-led initiative ensures that BankID aligns with the banking industry's need for secure and efficient identity verification processes. However, the public sector's role cannot be understated; Swedish governmental bodies interact closely with BankID to ensure that it meets national standards for security and privacy, aligning with regulations such as the EU's eIDAS framework and GDPR. This collaboration between public regulatory frameworks and private innovation allows BankID to serve as a critical infrastructure for digital transactions and identity verification across Sweden, integrating governmental services with private sector offerings. This governance model facilitates a robust and secure digital identity system, but it also raises considerations about potential biases towards banking functionalities and the dominance of major financial institutions in the system's ongoing development and accessibility.

Trust model of Sweden's BankID system

Sweden's BankID employs a centralized trust model that is built on a public key infrastructure (PKI), that employs asymmetric cryptography to secure the digital identities of users, where digital certificates, necessary for authentication and signing, are issued by trusted entities, primarily a consortium of major Swedish banks. The centralized nature of BankID means that these banks manage and control the issuance, renewal, and revocation of digital certificates, ensuring that all operations adhere to strict security and compliance standards set by both national and European regulations, such as the eIDAS framework.

This trust model positions the banks both as service providers and gatekeepers of security and identity verification, leveraging their natural advantage given by the trust they enjoy from the citizens and the high levels of due diligence that regulators require them to perform. While this centralized approach offers significant advantages in terms of reliability, consistency in user experience, and regulatory compliance, it also centralizes risk, making it critical to continuously evolve security measures to counter potential threats.

Despite the centralized control, BankID's infrastructure is robust, benefitting from the collective oversight and technological expertise of the participating banks, which helps maintain high levels of trust and operational integrity in the system.

Interoperability with other systems

BankID's design emphasizes interoperability, allowing it to function seamlessly with a wide range of public and private digital services: this interoperability is one of the main reasons for its widespread adoption, enabling users to access various online services with a single digital identity solution. BankID integrates with governmental platforms for e-services, various banking systems, and private sector services ranging from healthcare to online retailing. The system's ability to work across different platforms and service providers without compatibility issues is crucial for the digital ecosystem in Sweden, promoting a unified approach to digital identity that simplifies user interactions and enhances the overall efficiency of online services.

User Experience considerations

The user experience with BankID is designed to be straightforward, secure, and convenient, promoting widespread usage across various demographic groups in Sweden. Accessibility features are a significant focus, with the system offering different forms of digital IDs, as seen previously, to meet diverse user preferences and security needs. This flexibility allows individuals to choose the format that best suits their lifestyle and technical capabilities, enhancing the system's inclusivity. BankID's user interface is streamlined and intuitive, which minimizes the learning curve and reduces barriers to adoption. Moreover, continuous improvements are made to ensure the system remains user-friendly while incorporating advanced security measures to protect user data and prevent fraud.

Let's take the same use case presented for Estonia's eID: in this case the user has a BankID account and wants to apply for a loan. Let's differentiate between two situations: one where the user is applying for the loan on his laptop (case A) and another one where he is using the mobile banking app (case B). In the first case, for the user identity confirmation, the bank will require him to scan a QR code with his BankID app on the smartphone; then he will have to insert his security code in the app as well (or

alternatively use his face ID) and then go back to the bank website. In the second one, directly from the mobile banking app he will be redirected to the BankID interface and insert the security code/use face ID and finally go back to the previous app. The flow is illustrated in *Figure 5* below.

Factors contributing to the effectiveness of BankID

We can identify three main factors making BankID a foundation of Sweden's digital infrastructure and a model for digital identity systems globally, namely the robust banking partnerships that manage it, Swedish technological infrastructure and the widespread trust in financial institutions.

The development and ongoing enhancement of BankID have been enabled by strong collaborations among major Swedish banks, that constantly make sure that the system remains relevant and effective in addressing the needs of a dynamic financial services market. Moreover, the cooperative model allows for shared investment in technological advancements and security enhancements, making it a cost-effective solution for participating institutions.

BankID's can operate efficiently and securely across the country thanks to Sweden's advanced technological infrastructure, with high internet penetration and a strong digital framework.

Finally, Swedish citizens exhibit a high degree of trust in financial institutions, which has facilitated the acceptance and widespread use of BankID. The trust placed in these institutions extends to the digital tools they support, such as BankID, which is seen as an extension of the banks' commitment to secure and customer-friendly service. This cultural aspect is crucial, as it underpins the consumer willingness to engage with digital identities in their financial interactions, contributing significantly to the system's effectiveness.

By addressing both the operational needs of the banking sector and the consumer preferences for digital interaction, BankID exemplifies a successful integration of technology with financial services.

Figure 5: Screen example of BankID app usage to confirm identity while logging in to the bank.

Source: https://developer.signicat.com/identity-methods/sbid/about-sbid.html#use-cases

In the next section we are going to analyse a totally different country with its digital identity system, that will offer a completely different perspective: India with its Aadhaar.

5.1.3 India’s Aadhaar

5.1.3.1 Socio-economic context

Economic growth and sustainability

India, with a population of more than 1.4 billion people, is the largest democracy of the world with highly dynamic economy and complex social structure. Over the past decade, India's integration into the global economy has driven significant economic growth, positioning it as a key player on the international stage. The country's GDP growth rate, one of the highest in the world, that has withstood the impact of global financial fluctuations, is an evidence of its thriving market and the reformative government policies aimed at ensuring sustainable economic development. The economic reforms, such as the implementation of the Goods and Services Tax (GST) and corporate tax reductions, aimed to encourage investment and improve productivity, are some of the steps taken by the government to accelerate the economic growth. However, the public debt-to-GDP ratio remains high, and economic disparities persist, suggesting the need for sustained and inclusive economic policies that address both growth and socio-economic inequalities.

As one of the world's fastest-growing economies, India is trying to balance economic development and environmental sustainability. On the one hand, it aspires to achieve high middle-income status by the centenary of its independence in 2047; on the other, this ambition is matched by its commitment to sustainability, particularly its commitment to reach net-zero emissions by 2070. In fact, the environmental landscape in India is marked by severe challenges, including alarming levels of air pollution, and government initiatives aimed at increasing the renewable energy share in the energy mix to 40% and subsidizing clean gas connections are steps toward fostering green growth and mitigating climate change effects.

Digital governance and infrastructure

India's digital landscape has been significantly transformed by initiatives aimed at increasing digital access and government services' efficiency: for example, the national digital identity program, Aadhaar, is a pillar of India's digital governance, providing a unique identification number to over a billion citizens. This program, that contributes to the achievement of a more egalitarian society, since it is built with inclusive growth and equitable access to resources and opportunities in mind, supports India's digital infrastructure by facilitating access to public services, enhancing the efficiency of bureaucratic processes, and improving transparency in government interactions. Furthermore, the push towards digitalization is supported by substantial investments in internet connectivity and digital literacy programs, aimed at overcoming the huge digital divide across its vast and diverse population.

Market dynamics and global competitiveness

In the context of global economic integration, India has made notable advances, particularly in the information technology, pharmaceuticals, and manufacturing sectors. The IT sector, in particular, has positioned India as a global leader in software development and services, contributing significantly to its GDP and employment. Exports of pharmaceuticals have also grown significantly and India’s share in global trade is increasing.

Despite these achievements, India lags in market competitiveness because of regulatory constraints, infrastructural weakness and labour market rigidity: reducing trade barriers, modernizing labor laws, and enhancing infrastructural capacities are seen as critical steps towards boosting India’s competitive advantage in the global market.

Addressing extreme poverty, urban development and housing

Despite its economic achievements, India continues to face significant social challenges, including extreme poverty, inadequate urban development, and a critical housing shortage.

Significant advances have been made in reducing extreme poverty, with the share of the population living below the international poverty line of $2.15 per day (2017 PPP) halving between 2011 and 2019. Despite these gains, the pace of poverty reduction has

recently seen a slowdown, worsened by the COVID-19 pandemic but showing signs of recovery in the subsequent years. However, social challenges are still a huge problem deserving attention, as evidenced by the persistence of consumption inequality, captured by a Gini index of around 35, and high levels of child malnutrition.

Also, employment quality remains a concern, with low women's participation in the workforce and the prevalence of under-employment, highlighting the need for substantial job creation and real wage growth.

Urban development and housing remain critical areas of concern, with many households living in precarious conditions despite numerous housing initiatives. The government's "Housing for All" program launched in June 2015 underscores the efforts that had been made to tackle this issue by 2022, but challenges such as high construction costs and stringent zoning regulations have constituted a deterrent, particularly in urban centers where there is an imbalance between the demand for low-end housing and the supply of high-end one. More effective urban planning and investment in affordable housing are crucial for improving living conditions and supporting sustainable urban development.

Impact of India's diverse and populous landscape on digital identity needs

India's diverse and populous landscape significantly impacts its digital identity needs, making a universal and scalable solution like Aadhaar, India’s national digital identity system, not just beneficial but essential. The vast demographic expansion encompasses a wide range of socio-economic statuses, ethnicities, and cultures, each with unique identity verification and access needs. In fact, India has a wide economic disparity among its citizens; this ranges from very wealthy individuals and middle-class families to those living in poverty. Each group has different access to technology and financial services, which affects how they might use and access a digital identity system: for instance, rural and poorer populations might have less access to the necessary technology to register or use digital ID systems compared to urban populations. Moreover, India is ethnically diverse with numerous ethnic groups and indigenous populations, each with their own languages and a national digital identity system needs to be flexible enough to work across these various groups, accommodating different languages. Finally, cultural practices and norms can shape the way people interact with technology and government systems: some communities may have a lack of trust towards central authorities or may

not comprehend how digital systems work, which can affect their willingness to enroll in or use digital identities. Aadhaar, as a biometric-based digital identity system, provides a foundational platform that addresses these diverse requirements effectively.

The scalability of Aadhaar is crucial in a country where millions of people still lack access to formal identification: in fact, by providing a unique identifier that is linked to biometric data, Aadhaar ensures that even the most marginalized communities can access basic services, from banking and mobile connectivity to government welfare schemes and healthcare. This inclusivity is vital for driving financial inclusion and socio-economic participation across India's diverse population.

Moreover, the use of Aadhaar as an authenticating mechanism for various government and private services has led to process simplification, fraud reduction and efficiency gains, aligning with the government's Digital India[6] initiative aimed at transforming the nation into a digitally empowered society and knowledge economy.

5.1.3.2 India's Aadhaar system overview

Type of digital identity solution

Aadhaar, established by the Unique Identification Authority of India (UIDAI), provides a 12-digit unique identification number linked to an individual's biometric (such as fingerprints, iris scans and photograph) and demographic (such as name, gender, birth date and address) data. This system is primarily designed to ensure that every resident of India has a single, unique identity which can be used across many services.

At its core, Aadhaar employs a biometric system where each individual's biometric data are recorded. The system provides a web-based portal managed by UIDAI that allows users to apply for an Aadhaar number, download Aadhaar cards, update personal information, and check the status of their Aadhaar application. It is designed to be user-friendly and is accessible through standard web browsers, facilitating ease of access for users with internet connectivity.

[6] Digital India is a comprehensive government initiative launched in 2015 to transform India into a digitally empowered society and knowledge economy. It focuses on enhancing digital infrastructure, increasing internet access, and promoting digital literacy to improve public and government services. The initiative supports inclusive growth by integrating various government schemes and fostering innovation, aiming to connect rural areas with high-speed internet and make digital services accessible to all citizens.
Source: https://www.digitalindia.gov.in

To enhance accessibility and convenience, UIDAI has developed a mobile application called mAadhaar, available for both Android and iOS platforms, that enables users to carry a digital version of their Aadhaar card on their mobile devices: features include biometric locking/unlocking, viewing and sharing updated Aadhaar profile data, and generating/offline sharing of Aadhaar QR codes. The app is designed to work even on basic smartphones, expanding its reach to a larger segment of the Indian population.

Thanks to the multiple authentication APIs developed by Aadhaar, diverse service providers can use it for verifying the identity of users seamlessly: for example financial services providers can use it to perform know-your-customer procedures efficiently and without paperwork.

One of the significant strengths of Aadhaar is its inclusivity; the system, in fact, is designed to serve all residents of India, including those from rural and remote areas. Special mobile enrollment stations and camps are set up throughout the country to register individuals who might not have easy access to permanent enrollment centers.

The user interfaces of the UIDAI web portal and the mAadhaar app are designed to be simple and intuitive and instructions are available in multiple languages to address the diverse linguistic population of India, making the system accessible and easy to use for a broad audience.

Despite its wide reach, Aadhaar's digital solutions face challenges, particularly in rural areas where internet connectivity is poor or unreliable. Additionally, while biometric authentication enhances security, it can sometimes fail to recognize the registered biometrics of users, particularly the elderly and manual laborers, whose fingerprint quality may degrade over time.

Governance structure

Aadhaar is primarily developed and managed by UIDAI, which is a statutory authority established under the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. UIDAI operates under the Ministry of Electronics and Information Technology, Government of India. The development of the Aadhaar system, therefore, is firmly within the public sector's domain, emphasizing its role as a government-driven initiative.

As the main body responsible for the implementation and maintenance of the Aadhaar system, UIDAI handles all core aspects including policy formulation, Aadhaar enrollments, authentication services, and ensuring the security of stored biometric and demographic data. UIDAI's responsibilities include:

- issuance of Aadhaar numbers to residents,
- management of the Central Identities Data Repository (CIDR) where all resident data is stored,
- formulating policies and procedures for the safe and secure management of identity information,
- ensuring accessibility of Aadhaar for residents to facilitate benefits and services.

While the UIDAI is a public authority, it collaborates with various private sector entities for specific operational components: for example, it partners with enrollment agencies across the countries, that are private firms in charge of the physical process of enrolling residents into the Aadhaar system, by collecting their biometric and demographic data.

The technical infrastructure of Aadhaar, including software development and maintenance, involves collaboration with private tech companies, such as Infosys and other IT service providers.

Authentication User Agencies (AUAs) are typically private sector entities or government departments that use the Aadhaar authentication and e-KYC services provided by UIDAI to authenticate the identity of residents. This relationship allows for a wide range of services, from opening bank accounts to mobile phone connections, all leveraging the Aadhaar infrastructure.

The governance structure of Aadhaar is designed to ensure that UIDAI operates with transparency and accountability while protecting resident data. The Aadhaar Act provides a strong legal framework that dictates how Aadhaar data can be collected, used, and shared, and it also outlines penalties for misuse of data, aiming to safeguard privacy.

Being a government authority, UIDAI is subject to oversight by various governmental bodies, including the Supreme Court of India, which has already decided on many aspects of Aadhaar especially relating to data privacy and security.

All things considered, the Aadhaar system is primarily a public sector-driven initiative with significant collaboration with private sector partners for operational effectiveness and technological advancements. This hybrid model leverages the strengths of both

sectors: the public sector's ability to regulate and manage a national identity system on one hand, and the private sector's technological expertise and operational efficiency on the other. The governance structure ensures that while private entities contribute to the system's functionality, overall control and accountability remain with the public sector, thereby aiming to balance efficiency with the protection of residents' privacy and data security.

Trust model of Aadhaar: centralized database system

Aadhaar is built on a centralized database model managed by UIDAI, thus the trust model of the system is heavily reliant on government oversight and regulation.

All Aadhaar data, biometric and demographic details of residents, is stored in the CIDR, facilitating the unique identification of over a billion people and allowing for efficient querying and authentication requests to confirm identities.

The system uses a simple but robust authentication mechanism, whereby an individual's biometric data is compared against the stored records in the CIDR upon request. Authentication can be based on biometrics, an OTP received by text message, or demographic data, providing flexibility in how verification is performed.

Let's analyse a use case: a user with an associated Aadhaar identification number is entitled to get a scholarship from government welfare schemes and wants to request it. She first needs to authenticate to access the central government benefits and she chooses to do it through biometric authentication. The system encrypts the data, that go to the AUA to be signed and finally to the CIDR, that decrypts and validates them against its stored parameters, giving back a yes/no response. The flow is illustrated in Figure 6 below.

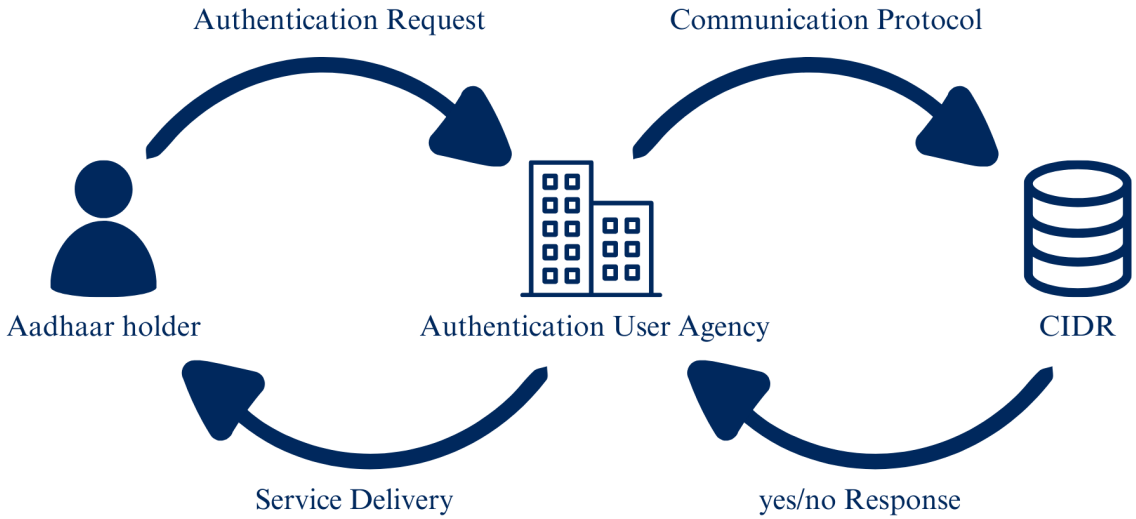

Figure 6: Simplified overview of Aadhaar authentication proccess.

The centralized nature of Aadhaar allows for high interoperability with various government and private systems. It facilitates straightforward integration across different platforms and services, making it easier for entities to leverage Aadhaar for identity verification.

While the centralized model offers significant benefits in terms of ease of access and efficiency, it also raises concerns regarding privacy and data security. The potential for misuse or unauthorized access to centralized databases is a significant issue, which has led to extensive judicial and public scrutiny in India. To this purpose, the Aadhaar Act includes provisions to safeguard personal data and restricts usage norms for third parties and UIDAI has implemented multiple layers of security to protect data stored in CIDR, including complex encryption and strict access controls. Regular audits and monitoring are part of the operational protocols to ensure data integrity and security.

Role in public welfare and services

Aadhaar has been a catalyst in improving the delivery and access to public service and welfare schemes in India. As a foundation of the government's Digital India initiative, unique identification provided by Aadhaar number offers a strong mechanism to ensure

that government subsidies, healthcare benefits, educational programs, and financial services meant for the poor and disadvantaged are delivered efficiently and transparently. By linking Aadhaar numbers to bank accounts, the government has streamlined the distribution of social welfare benefits through Direct Benefit Transfer (DBT), significantly reducing leakage and corruption in the system. The direct transfer of subsidies to beneficiaries' accounts precludes the involvement of intermediaries and ensures that the benefits are accessed only by the eligible beneficiaries. Further, the linkage of Aadhaar with bank accounts enables the government to track the benefits in real time and ensures an audit trail of money disbursed to beneficiaries.

Aadhaar's widespread acceptance across public service platforms has enabled citizens to access essential services with greater ease, without much bureaucratic procedures and delays, improving overall service delivery. This has been particularly impactful in rural and underserved areas, where Aadhaar has been instrumental in bringing a large segment of the population into the formal socio-economic framework, thus promoting inclusive growth and enhancing the scope of public welfare initiatives.

5.1.4 Singapore's SingPass

5.1.4.1 Socio-economic context

Economic development and growth

Singapore, a high-income city-state, is renowned for its remarkable transformation from a modest trading hub to a global financial center within just a few decades. Its strategic geographic location at the southern end of the Malay Peninsula has played a crucial role in its economic importance, especially as one of the world's busiest ports, linking the Indian Ocean to the South China Sea.

Since its independence in 1965, Singapore has followed a development strategy focused on export-oriented industrialization, using foreign investment and technology as the main engines of economic growth. As a result, Singapore is now one of the world's most

competitive economies, with a GDP per capita significantly higher than many of its Southeast Asian neighbors.

Manufacturing and services are the two key economic sectors of Singapore, with significant contributions from electronics, petrochemicals, and financial services. The government's proactive attitude in economic planning has led to the development of a robust regulatory and infrastructural framework that supports business activities, attracting a large number of multinational corporations to set up their business in the country.

Social policies and inequality

Despite its economic success, Singapore faces challenges related to social equality and inclusion: in fact, the government's rigorous meritocracy and high-performance standards have fostered a competitive environment that can exacerbate social disparities. While the Gini coefficient has seen moderate improvements in income inequality due to government transfers, disparities remain a concern.

The government addresses these challenges through various programs and initiatives, such as the SkillsFuture[7] one, aimed at lifelong learning and workforce upskilling.

Moreover, Singapore's approach to housing is a pillar of its social policies: the government, through the Housing and Development Board (HDB), has implemented an extensive public housing program that accommodates the majority of the population, in this way fostering community cohesion and trying to integrate different income and ethnic groups.

Urban planning in Singapore is carried out with utmost care and attention to optimize the use of limited land resources, balancing between industrial, residential, and green spaces. The government's forward-looking urban policies have made Singapore one of the most livable cities in Asia, with a high emphasis on sustainability and quality of life.

[7] SkillsFuture is a national initiative in Singapore aimed at promoting lifelong learning and skills mastery among Singaporeans, helping them to develop their potential and secure fulfilling careers in a future-ready economy. It focuses on continuous education and skills upgrading to meet evolving industry needs and enhance employability in a competitive global market.
Source: https://www.skillsfuture.gov.sg/aboutssg

Singapore's tech-forward approach: the Smart Nation initiative

Singapore's vision to be a "Smart Nation" exemplifies its tech-forward strategy. This initiative, launched by Prime Minister Lee Hsien Loong in 2014, is aimed at integrating technology into every aspect of life to enhance the city-state's urban environment and improve the quality of life for its citizens. It focuses on creating a digital-first society, economy, and government, enhancing services and lifestyles through digital solutions, fostering innovation, and ensuring cybersecurity and data privacy. This initiative also promotes international collaboration and aims to establish Singapore as a global model for smart urban development.

In the context of this program, Singapore has actively promoted the digitalization of its economy, encouraging critical sectors, including finance, healthcare, and education, to adopt innovative technologies such as Artificial Intelligence, Internet of Things, and Big Data analytics.

The government has transformed public service delivery through the use of technology, streamlining government interactions and making public services more accessible to citizens.

Singapore uses smart technology to optimize everything from traffic management to waste management and water conservation; IoT sensors and smart systems are deployed across the city to monitor and manage urban operations, reduce resource consumption, and improve environmental sustainability.

High governance standards

Singapore is recognized globally for its high governance standards, which are characterized by robust regulatory frameworks, transparency, and accountability.

Singapore has a reputation to be one of the least corrupt countries in the world, thanks to strict anti-corruption laws, transparent legal processes, and the Corrupt Practices Investigation Bureau's active enforcement policies.

The Singaporean bureaucracy is known for its efficiency and effectiveness, attributed to a meritocratic recruitment system and a competitive remuneration scheme that attracts top talents to the public sector.

The government continuously tests new ideas and technologies to come up with proactive and adaptive policies and, although known for its top-down governance approach, it

increasingly engages with stakeholders including businesses, academia, and civil society to inform policy-making, in order to shape more inclusive and effective governance.
This combination of a tech-forward approach and high governance standards lies at the basis of Singapore's strategy to maintain its economic dynamism and financial stability, ensuring its resilience against economic fluctuations and other global challenges.

5.1.4.2 Singapore's Signpass system overview

Singpass, which stands for Singapore Personal Access, is a national digital identity platform that facilitates secure and convenient access to both government and private sector services in Singapore. It has been developed and managed by the Government Technology Agency (GovTech) and is one of the many innovations promoted by Singapore's Smart Nation initiative, with the primary purpose is to streamline transactions and interactions with various services, enhancing the efficiency and ease of access for all users.

Type of digital identity solution
Singpass is a versatile digital identity system that incorporates both web-based and mobile-app-centric solutions: this dual-platform approach ensures broad accessibility and user adaptability, addressing diverse user preferences and technological access levels.
The Singpass system is accessible via a web portal, where users can log in using their unique credentials or through the Singpass mobile application, that enhances the user experience by leveraging mobile technology to offer additional features, such as QR code scanning and biometric authentications, like facial recognition and fingerprint scanning. The app is designed to be intuitive and user-friendly, ensuring that users can manage their digital identity and transactions effortlessly on their smartphones.
User experience is a central aspect of Singpass, influencing its design and ongoing development; in fact, the system is tailored to ensure ease of use, security, and accessibility, satisfying the needs of a diverse user base, including the elderly and people with disabilities.
Both the Singpass website and mobile app are designed with simplicity in mind, making navigation straightforward for all users. Moreover, the platforms support various

authentication methods, including QR code scans, SMS OTPs, and biometric options, which provide flexibility and enhance security.

As an example, the Singpass app includes features such as dark mode and compatibility with screen readers, which are beneficial for users with visual impairments.

Recognizing Singapore's multilingual society, Singpass is available in multiple languages, further improving accessibility and usability for a diverse user base.

Regular feedback loops through community engagement initiatives allow for continuous improvement of the UX, addressing user concerns and adapting to new user requirements as they arise.

Comprehensively, Singpass exemplifies an inclusive digital identity solution that integrates advanced technology with user-centric design principles, and the fact that it constantly gets enhanced and updated reflect Singapore's commitment to maintaining a leading edge in digital governance and citizen services.

Governance structure of Singpass

Singpass is primarily developed and managed by the GovTech of Singapore, a statutory board under the Prime Minister's Office: this collocates the Singpass system exactly within the competence of the public sector. GovTech is responsible for the design, implementation, and constant enhancement of Singpass, aligning it with national digital strategies and policies aimed at transforming Singapore into a Smart Nation.

The involvement of GovTech ensures that the identity wallet is closely integrated with public sector services and adheres to stringent security and data protection standards imposed by the government. This public sector-led approach emphasizes the system's role in serving public interests, including enhancing accessibility, security, and convenience for all citizens and residents.

Additionally, the management of Singpass by a public sector entity, with oversight and regulation by the Singapore government, minimizes commercial biases that might prioritize profit over user security and convenience.

While the development and management of Singpass are led by GovTech, there is significant collaboration with the private sector, particularly in extending the functionality and reach of the system into private services. For instance, Singpass allows users to access services from over 1,700 private sector entities: this integration is

facilitated through APIs that allow private companies to connect securely with the Singpass system to verify identities and provide services efficiently.

An example of such collaboration is the development of Singapore Financial Data Exchange (SGFinDex) platform, which is a public-private partnership involving GovTech, the Monetary Authority of Singapore (MAS), several major banks, and the Smart Nation and Digital Government Group (SNDGG): it uses the digital identity data from Singpass to allow individuals to access and manage their financial information across different institutions seamlessly.

The collaboration with the private sector is primarily oriented towards enhancing the utility and reach of Singpass without compromising on the privacy and security aspects governed by public sector policies. This collaborative approach helps balance the innovation and efficiency of private sector technologies with the robustness and reliability of public sector governance.

Underlying trust model of Singpass

Singpass operates primarily on a centralized model, where the GovTech of Singapore manages and controls the core data infrastructure.

The centralization of data allows for a robust and secure management structure but raises concerns about single points of failure and potential vulnerabilities to attacks or breaches. However, Singapore mitigates these risks through stringent security measures and regular system enhancements to safeguard data integrity and user privacy.

Singpass incorporates a PKI for secure digital transactions, that involves the use of cryptographic keys to secure electronic communications and provides a framework for digital signatures and certificates. This technology supports the trustworthiness of Singpass transactions, ensuring that all interactions are authenticated and that the identity of users is verified reliably.

Digital certificates issued by the National Certification Authority of Singapore authenticate the digital credentials of users, thereby reinforcing the security and reliability of the identity verification process. Additionally, Singpass employs advanced biometric verification technologies, such as facial recognition, to enhance user authentication, that add a layer of security by linking the physical presence of a user to their digital identity, making unauthorized access more challenging.

While the primary infrastructure of Singpass is centralized, there are components of the system that use decentralized elements: for example, the Singpass app allows users to store digital versions of identity documents locally on their devices, which can be presented when required without needing to access the central database all the time.
Furthermore, there is a growing interest in exploring blockchain technology to enhance the security and decentralization of digital identities: blockchain, in fact, could potentially be used to distribute the storage of identity data across a secure, immutable network, reducing reliance on centralized systems and increasing resilience against attacks.
The API Exchange (APEX) platform is another critical element of the Singpass model: it facilitates secure data sharing between government agencies and the private sector through APIs. This system supports a controlled and secure method for accessing and integrating data across various services, enhancing the system's flexibility and responsiveness to different service needs.

Regulatory compliance

Singpass operates within a stringent regulatory framework that ensures compliance with national and international standards and is critical for maintaining user trust and system integrity in digital transactions. The Personal Data Protection Act (PDPA) governs the collection, use, and disclosure of personal data by organizations, providing a baseline standard of protection that Singpass must adhere to. Additionally, Singpass transactions are secured under the Electronic Transactions Act, which legally recognizes electronic signatures and records, further enhancing the system’s regulatory compliance.

Interoperability with other systems

Singpass demonstrates a high degree of interoperability, connecting seamlessly with various government and private sector systems. This is facilitated through the use of the previously mentioned APEX platform, which allows different systems to communicate and share data effectively. Singpass's integration with over 1,700 entities, including government agencies, banks, and healthcare providers, exemplifies its capability to operate across diverse platforms, ensuring that users can access a wide range of services through a single digital identity.

All things considered, Singpass stands out as a comprehensive digital identity system that effectively integrates regulatory compliance, system interoperability, user-centered design, and a complex technological infrastructure. This integration ensures that Singpass meets the current needs of users and service providers and also that it is well-positioned to adapt to future challenges and innovations in the digital identity space.

5.2 Cross-case thematic analysis and synthesis of findings

The aim of this section is to identify convergent and divergent themes across the case studies of Estonia, Sweden, India, and Singapore. The analysis will specifically explore themes along three critical dimensions: trust establishment, credential sharing control, and accessibility assurance.

The goal is first to unveil both patterns and discrepancies among the case studies and then explore the relationship between the operational and functional aspects of digital identity systems and the broader socio-economic factors influencing their implementation and acceptance: this analysis will help us understand why certain digital identity strategies are more effective or preferred in specific national contexts and how these systems can be designed or modified to meet the unique needs of different populations.

5.2.1 Trust establishment

The establishment of trust is crucial in the development and deployment of digital identity systems, since it supports their widespread adoption and underpins their operational integrity and user acceptance.

Let’s identify convergent and divergent themes among Estonia's eID, Sweden's BankID, India's Aadhaar, and Singapore's Singpass on how they build and maintain trust.

Convergent themes

1. Utilization of Public Key Infrastructure (PKI)

Both Estonia's eID and Sweden's BankID prominently use PKI to manage digital certificates and cryptographic keys, ensuring the authenticity and integrity of transactions.

Singapore's Singpass also integrates PKI for similar purposes, highlighting a common reliance on this technology across systems developed in technologically advanced societies.

2. Regulatory compliance

All four systems adhere to strict national (and in some cases, international) regulations designed to safeguard personal data and ensure privacy. For instance, Estonia's eID complies with the EU's eIDAS and GDPR, while Singpass aligns with Singapore's Personal Data Protection Act.

Divergent themes

1. Centralized vs. decentralized data management

India's Aadhaar operates on a centralized model where all biometric and demographic data is stored in a single national database. This contrasts sharply with the more decentralized approaches observed in Estonia and Sweden, where data is managed across various systems with stringent access controls. The centralized model in Aadhaar can pose risks of single points of failure and potential large-scale data breaches, which are mitigated in decentralized systems through distributed risk.

2. Authentication Methods

While all systems employ robust authentication methods, the type and extent vary significantly. Aadhaar's reliance on biometric data for authentication is one of its most defining features, contrasting with BankID's and Singpass's use of multifactor authentication, including mobile devices and passwords. Estonia's eID also includes physical tokens (ID cards with electronic chips), adding a layer of security that differs from the mobile-centric approaches prevalent in Singapore and Sweden.

5.2.2 Credential sharing control

Managing and controlling the sharing of credentials are fundamental aspects of ensuring user privacy and maintaining the integrity of digital identity systems, since they prevent unauthorized access and misuse of personal data.

Let's identify convergent and divergent themes among Estonia's eID, Sweden's BankID, India's Aadhaar, and Singapore's Singpass on this matter.

Convergent themes

1. User consent mechanisms

All four systems require user consent for data sharing, a crucial feature that empowers users and reinforces the trustworthiness of the systems. Whether it's through explicit user interfaces or secure consent protocols, each system ensures that individuals have control over when and how their personal data is accessed and used. This complies with privacy regulations and addresses user concerns about data sovereignty.

2. Data minimization

A common strategy across the systems is the principle of data minimization. Each system strives to ensure that only the necessary information required for a particular transaction or service is shared. For instance, both BankID and Singpass allow for transactions where only age or eligibility is verified without disclosing full identity details. This practice minimizes the risk of data exposure and enhances user privacy.

3. Integration with broader services

The integration of these identity systems with broader government and commercial services also is a shared characteristic. Singpass and Aadhaar, in particular, are deeply integrated into a wide array of public and private services, making them pivotal to accessing everything from healthcare to financial services. This extensive integration necessitates robust data sharing controls to prevent unauthorized access across services.

Divergent themes

1. Granularity of control over data sharing

While all systems implement user consent, the granularity of control over what data is shared and with whom varies significantly. BankID and Singpass offer more detailed control mechanisms through their user interfaces, allowing users to manage permissions and view detailed logs of data access. In contrast, Aadhaar's user controls are primarily focused on biometric locking/unlocking, with less visibility into the specific data shared during transactions. Estonia's eID provides a balance, with user consent required at each transaction but less emphasis on managing ongoing consent settings.

2. Approach to biometric data

The management of biometric data highlights another area of divergence. Aadhaar's extensive use of biometric data for identity verification involves significant data sharing

controls to protect this sensitive information. Singpass also utilizes biometrics but primarily in the context of authentication for access to government services, not as widely for commercial transactions. In contrast, BankID and Estonia's eID use biometrics more selectively, primarily for high-security transactions or not at all, focusing instead on digital certificates and PINs for authentication.

5.2.3 Accessibility assurance

Accessibility assurance, meaning whether these systems are usable by a broad spectrum of the population or not, including those with varying levels of digital literacy, access to technology, and language proficiency, is a critical dimension in evaluating the effectiveness of digital identity systems.

Despite the different socio-economic and technological landscapes in each country, the analysis across these four digital identity systems highlights a strong commitment to accessibility, with significant efforts made to ensure that digital identity services are inclusive and available to all users..

Let's anyway identify which are the convergent themes among Estonia's eID, Sweden's BankID, India's Aadhaar, and Singapore's Singpass on how they manage accessibility.

Convergent themes

1. Multilingual support

Each of the digital identity systems recognizes the linguistic diversity of its population. For example, Estonia's eID and Singpass offer services in multiple languages, which is crucial in multicultural societies like Estonia and Singapore. Similarly, Aadhaar provides support in multiple Indian languages to address the country's diverse linguistic landscape, and BankID includes provisions for Sweden's significant immigrant population.

2. Technological inclusivity

All four systems demonstrate a commitment to being accessible across various technological platforms. Estonia's eID, Sweden's BankID, and Singapore's Singpass offer mobile and web-based solutions that cater to users with varying levels of access to technology. Aadhaar also provides multiple access modalities, including physical enrollment centers to get the identification number, ensuring reach across India's diverse socio-economic spectrum.

3. Support for digital literacy

Estonia, Singapore, Sweden, and India each implement initiatives, though varying in approach, to improve digital literacy, crucial for ensuring that all segments of the population can effectively use digital identity systems.

Below is a table summarizing the findings of the thematic analysis along the three specified dimensions.

	ESTONIA	**SWEDEN**	**INDIA**	**SINGAPORE**
1) Trust establishment				
Utilization of Public Key Infrastructure (PKI)	Yes	Yes	No	Yes
Regulatory compliance	eIDAS, GDPR	eIDAS, GDPR	Aadhaar Act	PDPA, Electronic Transactions Act
Centralized vs. Decentralized data management	Decentralized	Decentralized	Centralized	Primarily Centralized
Authentication methods	Multifactor (mobile devices, passwords, physical tokens)	Multifactor (mobile devices, passwords)	Biometric	Multifactor (mobile devices, passwords, biometrics)

2) Credential sharing control				
User consent mechanisms	Yes	Yes	Yes	Yes
Data minimization	Yes	Yes	Yes	Yes
Integration with broader services	Yes	Yes	Yes	Yes
Granularity of control over data sharing	Moderate	High	Low	High
Approach to biometric data	Selective	Selective	Extensive	Moderate
3) Accessibility assurance				
Multilingual support	Yes	Yes	Yes	Yes
Technological inclusivity	Mobile, web-based solutions	Mobile, web-based solutions	Multiple access modalities	Mobile, web-based solutions
Support for digital literacy	Yes	Yes	Yes	Yes

Table 3: table summarizing the findings of the thematic analysis along the dimensions of trust establishment, credential sharing control, and accessibility assurance.

5.3 Factors influencing success

In this section we are going to make a summary of the critical success factors for each digital identity model and how they relate to the specific socio-economic contexts in which they have been developed.

Estonia

Estonia has leveraged its small size and lean government to become a leader in digital innovation. The country's socio-economic strategy focuses on digital literacy and technological infrastructure, making it supportive for implementing advanced technologies like eID.

Estonia's eID identified critical success factors are the following:

- **Comprehensive regulatory compliance:** the system's alignment with EU's eIDAS and GDPR provides a strong legal framework that builds trust and ensures privacy.
- **Decentralized data management:** it enhances security and reduces risks associated with data breaches.
- **High digital literacy and public engagement:** the various effective national digital education programs facilitate widespread adoption and utilization.

Sweden

Sweden's mature banking sector and high level of trust in financial institutions provide a fertile ground for BankID's success. The country's emphasis on innovation and digital governance aligns with the system's technological advances and user-centric design.

Sweden's BankID identified critical success factors are the following:

- **Public-private collaboration:** the strong cooperation between major banks and the government facilitates widespread acceptance and integration into various services.
- **Comprehensive regulatory compliance:** analogously to Estonia's eID, the system's alignment with EU's eIDAS and GDPR provides a strong legal framework that builds trust and ensures privacy.

India

India's diverse and continuously expanding population requires a robust system that can reach every citizen, making Aadhaar's inclusive and scalable model a necessity. The

socio-economic need to rapidly enhance service delivery and improve financial inclusion drives the adoption of such a comprehensive identity system.

India's Aadhaar identified critical success factors are the following:

- **Centralized identity management:** considering the Indian context, this charachteristic reveals to be positive, since it facilitates scale and integration across a vast range of government and private services, crucial for a populous country.
- **Biometric authentication:** it addresses the challenge of providing unique identifiers to a large population with varying levels of documentation.
- **Focus on inclusivity:** it focuses on extensive outreach, such as the availability of physical enrollment centers that ensure accessibility even in remote areas.

Singapore

As a compact and technologically advanced city-state with a diverse population, Singapore's development strategy emphasizes efficiency, security, and comprehensive digital integration. Singpass supports this strategy by facilitating seamless access to a wide array of digital services, making it an essential tool for everyday life in a highly digital society.

Singapore's Singpass identified critical success factors are the following:

- **Integration with the government Smart Nation initiative:** Singpass is a pillar of Singapore's smart technology infrastructure, enhancing service efficiency and government interaction.
- **Multimodal authentication and advanced security:** this reflects Singapore's high standards for data security and technological innovation.
- **Deep integrated into a wide array of public and private services:** it enjoys an ecosystem of almost 2000 service providers.

5.4 Theory formulation: adaptable frameworks for digital identity systems

Building on the thematic analysis and the critical success factors identified in previous sections, this theory proposes several frameworks that can be tailored by other nations according to their socio-economic similarities with Estonia, Sweden, India, and

Singapore. These frameworks are designed to offer guidelines that can assist policymakers, technology experts, and regulators in developing effective and inclusive digital identity systems.

The first proposed framework is the *Highly digital, small population model* (Estonia model), tailored for small to medium-sized countries characterized by high digital literacy, robust technological infrastructure, and proactive digital governance, that are looking to enhance their digital governance without the scalability challenges faced by larger countries. It focuses on leveraging these attributes to create a responsive and secure digital identity system that is also capable of offering valuable cross-border services. The key features are a decentralized data management system that enhances security and reduces systemic risks and adherence to international standards to ensure data protection and user privacy.

Let’s analyse each of them more closely.

In smaller countries like Estonia, decentralized data management allows for more agile and localized oversight of data, which is easier to manage and adapt than in larger, centralized systems. This flexibility enhances the system's resilience and responsiveness to specific community needs and technological changes. Moreover, by distributing data across multiple systems, the risk of large-scale breaches and operational failures is minimized, enhancing overall system security and reliability.

Estonia's compliance with EU standards such as eIDAS not only aligns with rigorous data protection and privacy norms but also facilitates the interoperability of Estonia’s eID across the European Union: this is essential for ensuring that Estonian citizens and businesses can easily access services throughout the EU, promoting economic activity and mobility. Adherence to these standards results in high domestic user trust and enhances Estonia's reputation on the international stage, promoting collaborations and trust with other nations and international bodies.

The second proposed framework is the *Collaborative, trust-based model* (Sweden model), particularly suited for countries where the financial sector is highly developed and trusted by the citizens. It capitalizes on the existing infrastructure and customer

relationships of financial institutions to facilitate a smooth introduction and operation of digital identity systems.

This model emphasizes the role of financial services providers in managing and implementing digital identity systems; in fact, these institutions bring a high degree of expertise in managing secure transactions and customer data and since citizens already place significant trust in their banking systems, leveraging this trust helps to ensure high user acceptance and widespread adoption of the digital identity system.

In this case, the system not only adheres to national digital identity regulations but also to stringent banking regulations, which demand rigorous security measures and data protections. This dual compliance ensures an added layer of system robustness and security.

Large population, inclusive model (India model) is the third framework, designed for populous developing countries characterized by significant diversity and varied levels of technology access, aiming to enhance social inclusion and digital accessibility. This model is characterized by a centralized system, which efficiently manages and integrates as efficiently as possible a vast array of data and services across a large population. The centralized nature allows for easier integration of the digital identity system with a wide range of services, from government subsidies to healthcare, ensuring that all citizens can access these services through a single identity proof.

Another key feature of this model is its reliance on biometric authentication, which allows to effectively handle identity verification across a large and diverse population base with varying levels of literacy and document accessibility, where other forms of identity verification might be less reliable or harder to implement.

Moreover, the model emphasizes accessibility by offering both physical and digital means to interact with the identity system: this dual approach ensures that individuals who lack digital access or prefer traditional methods can still engage with the system. Providing physical and widespread enrollment centers alongside digital services, for example, ensures that the system is inclusive and accessible to all citizens, regardless of their digital literacy or technological access.

The last framework is the *Technologically advanced, city-state model* (Singapore model),

tailored for small, technologically advanced nations or regions that prioritize digital transformation and smart governance. This model promotes a digital identity system that is deeply integrated with national digital strategies, such as smart nation or smart city programs, ensuring that the digital identity system functions as a core component of broader technological and administrative reforms.

A defining feature of this framework is its comprehensive integration across both public and private sectors, that facilitates seamless service delivery, greatly enhancing efficiency and improving the user experience. By connecting various services through a single digital identity platform, the system simplifies interactions for users and increases operational efficiency for service providers.

Furthermore, the model adheres to high security standards, implementing rigorous data protection measures to safeguard personal information: this is critical in maintaining trust among users, particularly in a highly connected environment where security concerns are prioritised.

For each model, the theory also proposes some implementation guidelines to ensure effective adaptation and operational success. In fact, it is strongly suggested that the countries concerned engage all relevant stakeholders including government, private sector, and civil society to align goals and ensure broad initiative support. Moreover, they should first initiate pilot projects to test the framework in localized settings before a full-scale rollout. Finally, it is fundamental to regularly evaluate the performance and societal impact of the implemented system and make adjustments when necessary based on technological advances and changes in socio-economic conditions.

These adaptable frameworks provide a structured approach for other countries to consider when developing or refining their digital identity systems. By aligning with socio-economic conditions similar to those of Estonia, Sweden, India, or Singapore, countries can leverage proven strategies and adapt them to meet their specific needs and challenges.

CHAPTER 6: IMPLICATIONS, LIMITATIONS, AND CONCLUSIONS

This research has led to the development of a theoretical framework for digital identity systems, tailored to various socio-economic contexts as exemplified by Estonia, Sweden, India, and Singapore, designed to guide policymakers, system designers, and other stakeholders in creating or refining digital identity systems that are secure, inclusive, and effective.

In this final chapter we are going to summarise the theoretical and practical implications of this theory, position Italy within the proposed models, and outline the limitations of the study while suggesting areas for further research.

6.1 Theoretical implications

This research aimed to explore how current successful digital identity wallet solutions align with institutional structures and digital strategies at the country level, and how these systems balance security, privacy, and user experience within their specific socio-economic contexts, ultimately developing a contingency theory for digital identity systems. The findings from this research have significant theoretical implications, contributing to the broader academic discourse on digital identity and technology implementation. Let's look at them more closely.

Alignment with institutional structures and digital strategies

The analysis of Estonia, Sweden, India, and Singapore has allowed us to gain an in-depth understanding of how digital identity systems align with their respective institutional structures and digital strategies, since it has been analysed how each country's approach reflects its unique socio-economic environment, technological infrastructure, and cultural attitudes.

The Estonian eID system's success is closely tied to its centralized yet distributed data management approach, which is well-suited to the country's high level of digital literacy and robust technological infrastructure. The alignment with EU regulations like eIDAS and GDPR further ensures a strong legal framework that builds trust and ensures privacy.
The Swedish BankID system exemplifies a successful public-private partnership, leveraging the trust and infrastructure of the financial sector. Sweden's emphasis on innovation and digital governance supports the widespread adoption and integration of BankID into various services. This model shows how leveraging existing trusted institutions can facilitate the acceptance and efficacy of digital identity systems.
Indian Aadhaar's centralized system addresses the need for a scalable solution in a highly populous and diverse country. Its reliance on biometric authentication ensures that even those without traditional documentation can access essential services. This system's success underscores the importance of inclusivity and accessibility in digital identity implementations in developing countries.
Singapore's Singpass is deeply integrated into the government-sponsored Smart Nation initiative, reflecting the city-state's emphasis on efficiency, security, and comprehensive digital integration. The high standards for data security and technological innovation in Singapore are critical to the system's effectiveness and trustworthiness.
In conclusion, these case studies have collectively illustrated that digital identity systems, to be successful, must be tailored to fit the specific socio-economic and institutional contexts in which they are implemented, answering the research question formulated in Chapter 3.

Expanding contingency theory to federated digital identity systems

This research contributes to the broader academic knowledge by extending the application of contingency theory to digital identity systems: traditionally applied in organizational studies, contingency theory suggests that a leader's optimal course of action and success depends on the internal (organization-specific) and external (related to the surrounding environment) circumnstances; by extending this theory to digital identity systems, the research provides a framework for understanding how socio-economic factors influence the success of technology implementations in this field.

The study highlights how factors such as technological infrastructure, cultural attitudes towards privacy, and levels of digital literacy significantly impact the design and implementation of digital identity systems. For instance, the high digital literacy in Estonia supports the effective use of a sophisticated eID system, while India's Aadhaar system addresses low literacy and varying documentation levels through biometric identification.

Additionally, the findings underscore the idea that there is no universal solution for digital identity systems: the optimal design and implementation strategies are contingent upon specific contextual factors. This reinforces the need for policymakers and system designers to consider these factors when developing digital identity solutions.

The proposed adaptable frameworks for digital identity systems based on the case studies provide practical guidelines for other countries and can help policymakers design systems that are effective within their specific socio-economic contexts, enhancing the overall success of digital identity implementations.

Implications for practice and future research

The theoretical implications of this research have several practical applications; in fact, policymakers can use the findings to develop digital identity systems that are tailored to their country's specific needs, since the proposed frameworks offer a starting point for designing systems that balance security, privacy, and user experience.

Future research can build on these findings by exploring additional case studies and further refining the proposed frameworks. There is also potential for examining the long-term impacts of digital identity systems on socio-economic development.

Finally, investigating how emerging technologies, such as blockchain and artificial intelligence, can enhance digital identity systems will be a valuable area of study.

We are going to deepen all these aspects in the following section.

6.2 Practical implications

This section will outline practical implications for stakeholders and, as an example, position Italy within the proposed theoretical framework, offering actionable insights for the development of its digital identity system.

Guidance for policymakers and system designers

To identify the most suitable model from the proposed frameworks, policymakers involved in the planning or refinement of digital identity systems should start by assessing the existing technological infrastructure, digital literacy levels, and cultural attitudes toward privacy in their country.

An aspect that has emerged regarding the tailoring of the systems to socio-economic contexts is inclusivity and accessibility; in fact, ensuring that digital identity systems are inclusive and accessible to all citizens is crucial: this involves considering factors such as internet penetration, access to digital devices, and the socio-economic diversity of the population. Systems like India's Aadhaar demonstrate the importance of providing both digital and physical enrollment options to ensure broad accessibility.

Finally, the implementation of robust security measures and adherence to data protection regulations are essential to build trust among users. Systems should incorporate advanced technologies like PKI and biometric authentication while ensuring compliance with national and international standards.

For what concerns stakeholders' engagement, successful digital identity systems, such as Sweden's BankID, highlight the importance of collaboration between public and private sectors: policymakers should foster partnerships with financial institutions, technology companies, and other stakeholders to leverage their expertise and infrastructure.

Also, engaging with the community through public consultations and feedback mechanisms can help in understanding user needs and addressing concerns: this approach would ensure that the system is user-friendly and aligned with the expectations of the citizens.

Before full-scale implementation, policymakers should initiate pilot projects to test the digital identity system in localized settings, that can provide valuable insights into the system's functionality, user acceptance, and potential challenges. Then, based on

feedback from pilot projects and ongoing user experiences, continuous improvements should be made to enhance the system's usability, security, and accessibility. This iterative approach ensures that the digital identity system remains relevant and effective over time.

Positioning Italy within the theoretical framework

Italy is in the process of developing its IT Wallet, as discussed in Chapter 2.

To position Italy within the theoretical framework developed in this research, it is essential to analyze its socio-economic context and current digital identity initiatives in light of the findings.

Italy has a well-developed technological infrastructure, but there are disparities in internet access between urban and rural areas: this suggests the need for a model that ensures inclusivity across different regions.

Moreover, the level of digital literacy in Italy varies, with significant portions of the population still needing support to navigate digital services effectively: hence, initiatives to enhance digital literacy should be integral to the development of the IT Wallet.

As evidenced by the robust data protection laws in place, aligned with the EU's GDPR, and the scrupulous work done by the Italian Data Protection Authority (*Garante per la protezione dei dati personali*) in enforcing these laws, we can affirm that Italy places a great importance on privacy and Italians are generally concerned about it, indicating the importance of robust data protection measures and transparent practices to build trust in the IT Wallet.

Given Italy's mixed socio-economic context, a combination of the Estonia and Sweden models may be most appropriate: Italy could leverage its existing public and private sector infrastructures, while also ensuring robust regulatory compliance and data protection.

Italy should foster strong collaborations between government agencies, financial institutions, and technology companies to develop the IT Wallet, to leverage the strengths of each sector, ensuring a secure and efficient system.

To address regional disparities in digital access, instead, Italy should implement multiple access modalities, including both digital and physical enrollment options, similar to India's Aadhaar system, to ensure that all citizens, regardless of their technological access, can obtain and use the IT Wallet.

Emphasizing security and privacy, the IT Wallet should incorporate advanced encryption technologies, multifactor authentication, and compliance with EU regulations: this will help in building trust and ensuring the protection of personal data.
Italy should initiate pilot projects in different regions, especially focusing on rural and less connected areas, to gather insights, address specific challenges and refine the IT Wallet before a nationwide rollout. Establishing mechanisms for continuous user feedback and iterative improvements will ensure that the IT Wallet evolves in response to user needs and technological advancements.
All things considered, by applying the insights from this research, Italy can develop a robust and inclusive digital identity system that aligns with its unique socio-economic context.

6.3 Limitations and further research

Limitations of the study
While this research has provided valuable insights and a theoretical framework for digital identity systems tailored to specific socio-economic contexts, several limitations must be acknowledged.
The first identified one is the performed single-country analysis for each model; in fact, the theoretical framework developed in this study is based on the analysis of a single country for each proposed model, and, while these countries provide diverse and informative case studies, the generalizability of the models could be limited. Including multiple countries with similar socio-economic contexts but different digital identity systems would have strengthened the validity and reliability of the models.
The second one concerns the great rapidity of technological advancements: the field of digital identity is rapidly evolving, with continuous advancements in technologies such as blockchain, biometrics, and artificial intelligence. The models developed in this study may quickly become outdated as new technologies emerge and are adopted; therefore, the applicability of the findings might be limited over time, requiring ongoing updates and revisions to remain relevant.

Finally, the regulatory environment for digital identity systems is complex and subject to change: new laws and regulations, particularly concerning data protection and privacy, can impact the implementation and operation of digital identity systems. This study's models are based on current regulatory frameworks, and future changes could alter their applicability and effectiveness.

Recommendations for further research

To build on the findings of this research and address its limitations, the following areas are recommended for further investigation:

1. Broaden the analysis through comparative studies across multiple countries: future research should include comparative studies across multiple countries within each socio-economic category. By examining several countries with different digital identity systems but similar socio-economic contexts, researchers can identify commonalities and differences that provide a more robust foundation for the developed theoretical models.
2. Longitudinal studies to track changes over time: longitudinal studies that track the development, implementation, and impact of digital identity systems over time would provide deeper insights into their long-term effectiveness and adaptability. This approach can help identify trends, challenges, and best practices that evolve with technological and regulatory changes.
3. Evaluation of the impact of emerging technologies: as new technologies emerge, research should evaluate their potential impact on digital identity systems. Exploring how innovations such as decentralized identity, blockchain, and AI-driven security measures can be integrated into existing frameworks will be fundamental for developing next-generation digital identity solutions.
4. Exploring organizational-level digital identity solutions: it would be useful to investigate also digital identity solutions developed within companies or organizations, such as the United Nations Joint Staff Pension Fund's biometric and blockchain-based one, developed within the UN Digital ID programme to provide UN personnel with a digital identity and enhance administrative processes and efficiency. Examining such organizational-level implementations can provide insights into innovative solutions and best practices that can be applied at a

national level, offering a different perspective on the scalability and adaptability of digital identity systems.

By addressing these areas in future research, scholars and practitioners can develop more comprehensive, adaptable, and effective digital identity systems that are capable of meeting the diverse needs of global populations in an ever-changing technological landscape.

6.4 Conclusions

The development of digital identity systems is a critical component of modern governance and socio-economic development and, as nations increasingly move towards digital transformation, understanding the intricate relationship between digital identity systems and socio-economic contexts is essential in order to implement successful systems from the beginning.

This thesis has provided a theoretical framework that not only enhances academic understanding but also offers practical guidance for developing inclusive, secure, and effective digital identity solutions tailored to the unique needs of different populations. The journey towards robust digital identity systems is ongoing, and this research serves as a foundational step in guiding future innovations and implementations in this vital area.

BIBLIOGRAPHY

Abraham, A., Schinnerl, C., & More, S. (2021). SSI Strong Authentication using a Mobile-Phone based Identity Wallet reaching a High Level of Assurance. In *Proceedings of the 8th International Conference on Security and Cryptography (SECRYPT 2021)* (Vol. 1: SECRYPT, pp. 137-148). SciTePress. Available at: https://doi.org/10.5220/0010542801370148

Anand, N. (2021). *New Principles for Governing Aadhaar: Improving Access and Inclusion, Privacy, Security, and Identity Management*. In: Journal of Science Policy & Governance, Vol. 18, Issue 1. Available at: https://doi.org/10.38126/JSPG180101

Bogdan, S. (2021). *The European Digital Identity Framework*. Available at: https://www.worldbank.org/content/dam/photos/1440x300/2022/feb/eID_WB_presentation_BS.pdf

Czerny, R., Kollmann, C. P., Podgorelec, B., Prünster, B., & Zefferer, T. (2023). *Smoothing the Ride: Providing a Seamless Upgrade Path from Established Cross-Border eID Workflows Towards eID Wallet Systems.* In S. De Capitani di Vimercati, & P. Samarati (Eds.), SECRYPT 2023 - Proceedings of the 20th International Conference on Security and Cryptography (Vol. 1, pp. 460-468). (Proceedings of the International Conference on Security and Cryptography; Vol. 1). SciTePress. Available at: https://pure.tugraz.at/ws/portalfiles/portal/63222089/SECRYPT_2023_96_CR_7.pdf

Dib, O., Toumi, K. (2020). *Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions.* In Annals of Emerging Technologies in Computing, pp. 19-40, Vol. 4, No. 5, Published by International Association of Educators and Researchers (IAER). Available at: https://ssrn.com/abstract=3785452

Enterprise Estonia. *e-Identity*. Available at: https://e-estonia.com/solutions/estonian-e-identity/id-card/

Elsevier (2008). *STORK project takes flight in the EU*. Card Technology Today, Volume 20, Issue 6, Page 1. Available at: https://doi.org/10.1016/S0965-2590(08)70139-7

European Commission (2015). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: A Digital Single Market Strategy for Europe.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0192

European Commission (2021). *COM/2021/281 final: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0281

European commission (2023-a). *The common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework*. Available at: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

European commission (2023-b). *Estonia: Political, social and economic background and trends*. Available at: https://eurydice.eacea.ec.europa.eu/national-education-systems/estonia/political-social-and-economic-background-and-trends

European commission (2023-c). *Sweden: Political, social and economic background and trends*. Available at: https://eurydice.eacea.ec.europa.eu/national-education-systems/sweden/historical-development

European commission (2023-d). *2023 Country Report Estonia*. Available at: https://economy-finance.ec.europa.eu/system/files/2023-06/ip230_en.pdf

European commission (2023-e). *2023 Country Report Sweden*. Available at: https://economy-finance.ec.europa.eu/document/download/f1be28a3-7a04-40ff-9cf5-a2d007ca1f12_en?filename=ip251_en.pdf

Grönlund, Å. (2010). *Electronic identity management in Sweden: governance of a market approach.* In: Identity in the Information Society, Volume 3, pages 195–211 (2010). Available at: https://doi.org/10.1007/s12394-010-0043-1

Kallinikos et Al. (2022). *The Platformization of Banking: The Case of Flowe*. Available at: https://luissuniversitypress.it/wp-content/uploads/2022/03/Alaimo_Kallinikos_Sannino_case.pdf

Krauß, A.M., Kostic, S., Sellung, R.A. (2023). *A more User-Friendly Digital Wallet? User Scenarios of a Future Wallet.* Open Identity Summit 2023. Available at: https://doi.org/10.18420/OID2023_06

Leinbach, T.R. , Ho, R., Kennard, A., Winstedt, R.O. (2024). *Singapore*. Encyclopedia Britannica. https://www.britannica.com/place/Singapore

Lewan, M. (2018). *The Internet as an enabler of FinTech*. In: The Rise and Development of FinTech, Chapter 10. Available at: https://www.researchgate.net/publication/330897128_The_Internet_as_an_enabler_of_FinTech_chapter_10_in_'The_Rise_and_Development_of_Fintech'

Lips, S., Tsap, V., Bharosa, N., Krimmer, R., Tammet, T., Draheim, D., (2023). *Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership: Learning from the Case of Estonia.* In: Information Systems

Frontiers, Volume 25, pages 2439–2456. Available at: https://doi.org/10.1007/s10796-022-10363-5

Lukkien, B., Bharosa, N., De Reuver, M (2023). *Barriers for developing and launching digital identity wallets.* In Proceedings of the 24th Annual International Conference on Digital Government Research (DGO '23). Association for Computing Machinery, New York, NY, USA, 289–299. Available at: https://doi.org/10.1145/3598469.3598501

Majumdar, R. (2024). *India economic outlook, April 2024*. Deloitte Global Economics Research Center. Available at: https://www2.deloitte.com/us/en/insights/economy/asia-pacific/india-economic-outlook.html

McKinsey Global Institute (2019). *Digital identification: A key to inclusive growth*. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

MC, A., Shanmugam, K. (2023). *Implementing unique identification technology: The journey and success story of Aadhaar in India*. In: Journal of Information Technology. Available at: http://dx.doi.org/10.1177/20438869231200286

Mukhopadhyay, S., Bouwman, H., Jaiswal, M.P. (2019). *An open platform centric approach for scalable government service delivery to the poor: The Aadhaar case*. In: Government Information Quarterly, Volume 36, Issue 3, Pages 437-448. Available at: https://doi.org/10.1016/j.giq.2019.05.001

Nordic Institute For Interoperability Solutions. *X-Road. The free and open-source data exchange solution.* Available at: https://x-road.global

OECD (2023). *OECD Economic Survey. SWEDEN 2023. Executive Summary.* Available at:

https://issuu.com/oecd.publishing/docs/brochure_sweden_oecd_2023_economic_survey

OECD (2024-a). *OECD Economic Survey. ESTONIA 2024. Executive Summary.* Available at: https://issuu.com/oecd.publishing/docs/estonia_brochure_2024.final

OECD (2024-b). *India*. In: OECD Economic Outlook, Volume 2024 Issue 1: Preliminary version. OECD Publishing. Available at: https://www.oecd-ilibrary.org/sites/69a0c310-en/1/3/2/23/index.html?itemId=/content/publication/69a0c310-en&_csp_=3184060ecf59639d0f609174b10264b5&itemIGO=oecd&itemContentType=book

Privacy International (2021). *ID systems analysed: Aadhaar*. Available at: https://privacyinternational.org/case-study/4698/id-systems-analysed-aadhaar

Republic of Estonia Ministry of Economic Affairs and Communications (2021). *Estonia's Digital Agenda 2030*. Available at: https://www.mkm.ee/en/e-state-and-connectivity/digital-agenda-2030

Schwalm, S. (2023). *The possible impact s of the eIDAS 2.0 digital identity approach in Germany and Europe.* Open Identity Summit 2023. Available at: https://doi.org/10.18420/OID2023_09

Sellung, R., Kubach, M. (2023). *Research on User Experience for Digital IdentityWallets: State-of-the-Art and Recommendations.* Open Identity Summit 2023. Available at: https://doi.org/10.18420/OID2023_03

Söderström, F., Melin, U. (2012). *The Emergence of a National eID Solution : an Actor-Network Perspective.* Presented at the 35th Information Systems Research Seminar in Scandinavia – IRIS 2012, August 17–20, 2012, Sigtuna, Sweden. Available at: https://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-81083

Sullivan, Clare (2018). *Digital identity – From emergent legal concept to new reality*. Computer Law & Security Review, Volume 34, Issue 4. Available at: https://doi.org/10.1016/j.clsr.2018.05.015

The European Parliament and the Council of the European Union (1999). *DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures*. Available at: http://data.europa.eu/eli/dir/1999/93/oj

The European Parliament and the Council of the European Union (2014). *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910

The European Parliament and the Council of the European Union (2015). *DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance).* Available at: https://eur-lex.europa.eu/eli/dir/2015/2366/oj

The European Parliament and the Council of the European Union (2022 – a). *REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance).* Available at: http://data.europa.eu/eli/reg/2022/1925/oj

The European Parliament and the Council of the European Union (2022 – b). *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)*. Available at: http://data.europa.eu/eli/reg/2022/2065/oj

The World Bank Group (2021). *ID4D Global Dataset*. Available at: https://id4d.worldbank.org/global-dataset

The World Bank Group (2023). *The World Bank In India*. Available at: https://www.worldbank.org/en/country/india/overview

Tsap, V., Lips, S., Draheim, D. (2020). *Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia.* In: Kő, A., Francesconi, E., Kotsis, G., Tjoa, A., Khalil, I. (eds) Electronic Government and the Information Systems Perspective. EGOVIS 2020. Springer, Cham. Available at: https://doi.org/10.1007/978-3-030-58957-8_12

World Bank (2019). *World Development Report 2019: The Changing Nature of Work.* Washington, D.C.: The World Bank, p. 56. Available at: https://documents1.worldbank.org/curated/en/816281518818814423/pdf/Main-Report.pdf

World Bank (2020). *Estonia Human Capital Index 2020*. Available at: https://databankfiles.worldbank.org/public/ddpext_download/hci/HCI_2pager_EST.pdf

World Bank (2020). *Sweden Human Capital Index 2020*. Available at: https://databankfiles.worldbank.org/public/ddpext_download/hci/HCI_2pager_SWE.pdf

World Bank (2022). *National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX*. Available at: http://hdl.handle.net/10986/38201