Co-funded by the
Erasmus+ Programme
of the European Union

Diffusion of a national solution for digital identity in India – Comparison with European initiatives

MASTERTHESIS
to obtain the Erasmus Mundus Joint Master Degree

in Digital Communication Leadership (DCLead)

of

Faculty of Cultural and Social Sciences
Paris Lodron University of Salzburg

Technical Faculty of IT and Design
Aalborg University in Copenhagen

Submitted by
Umesh Sanjay Torawane
12046518
S1081913@stud.sbg.ac.at, utoraw21@student.aau.dk
Rebaek Sopark 5, Hvidovre 2650, Copenhagen
Denmark

Internal Supervisor: Reza Tadayoni
External Supervisor: Josef Trappel
Tutors: Henning Olesen & Franz Wolfhagen (IBM)

Department of Communication Studies

Salzburg, 22 May 2023

Preface

This document is a result of my 4 months master thesis which marks the completion of my Master's in Digital Communication Leadership. After working for several years in the industry I decided to peruse a master's course to expand my knowledge and also to experience life in a new country. Now that I am at the end of this course, I can very well say that I have achieved both my goals.

My desire to work towards a safer digital society is what led me to take up this thesis topic. Having worked on Identity and access management domain in my early career, this research seemed to blend perfectly where I could apply concepts from my previous work experience and knowledge from academics.

While I am the author of this report, it would not have been possible if I had not been surrounded by some fantastic people. They pushed me to achieve my goals and cheered as I inched closer to finish.

Firstly, I would like to thank IBM for giving me an opportunity to perform this research work under the mentorship of Franz Wolfhagen. He ensured that the research started on the right track and enabled me with opportunities beyond this work. Even though our conversations were sporadic, they enabled me to maintain focus on the essential aspects. I would also like to thank other colleagues at IBM who gave their valuable feedback on this research.

Next, I would like to acknowledge Aalborg University for providing an environment in which students are guided well during their thesis research and studies as a whole. The guidance outside of academics is equally important to complete studies which I could easily find in this university. For my thesis, I was lucky to be supervised by three very accomplished academicians – Prof. Reza Tadayoni, Prof. Henning Olesen, and Prof. Josef Trappel. They guided my research to ensure that it is completed on time and with high academic standards.

I hope that you would enjoy reading this document as much as I enjoyed making it.

Executive Summary

Digital identity solutions are systems that allow individuals to prove their identity digitally, without the need for physical documents or in-person verification. These solutions can take various forms, such as government-issued ID cards, biometric authentication systems, or digital certificates. In recent years, there has been a growing trend towards the adoption of national digital identity solutions in both developed and developing countries. This research aims to compare the implementation and effectiveness of these solutions in both types of countries and find an effective implementation strategy for developing countries.

In developed countries, national digital identity solutions are often implemented as a means to improve the efficiency and security of government services. For example, a digital identity system may be used to allow citizens to access their tax records or apply for social benefits online. These systems may also be used to improve security by enabling the use of strong authentication methods, such as biometrics or multi-factor authentication.

In developing countries, national digital identity solutions may be implemented for a variety of reasons, including to increase financial inclusion and improve the delivery of social services. For example, a digital identity system may be used to provide individuals with a secure and reliable way to access financial services, such as bank accounts or loans. These systems may also be used to improve the delivery of social services, such as healthcare or education, by enabling efficient and accurate targeting of beneficiaries.

The adoption of national digital identity solutions can have numerous benefits, including increased efficiency, security, and inclusion. However, the implementation of these systems can also be complex and may require significant investments in technology and infrastructure. It is important for governments and other stakeholders to carefully consider the costs and benefits of these systems, as well as the potential risks and challenges, before implementing a national digital identity solution.

Table of Contents

List of Table

Table of Figures

1. Introduction

1.1. Problem and Background

Identification in a digital age matters because it reduces complex humans to records and systems, mostly categorized by others. The term digital identity indicates the conversion of human identities into machine-readable digital data (Masiero & Bailur, 2021). Most nations, both developed and developing, now have digital identity schemes as part of their e-government initiatives and many have expanded to use the same identity for both public and private sector transactions (Sullivan, 2018). But developed countries have been way ahead as compared to developing countries when it comes to full-fledged utilization of digital identities. The range of potential value depends on the portion of economic activity where digital ID–based use cases could be deployed to address bottlenecks and inefficiencies, as well as the scope for improvement in formalization, inclusion, and digitization over current levels (Sullivan, 2018). Based on these considerations, we estimate that among emerging economies, the average country could achieve an economic value equivalent to 6 percent of GDP in 2030, while in mature economies, the average country could achieve an economic value equivalent to roughly 3 percent both assuming high levels of adoption and use in multiple domains (White & Madgavkar, 2019). India's Aadhaar system achieved over 90 percent coverage yet even in India, digital ID addresses a relatively small portion of the potential use cases (White & Madgavkar, 2019). Digital ID can help enforce rights nominally enshrined in law, for example, in India, the right of residents to claim subsidized food through ration shops is protected because their identity and claims are authenticated through a remote digital ID system, rather than at the discretion of local officials (White & Madgavkar, 2019). By providing greater legal protection, digital ID could help in the elimination of child labor, currently estimated to affect 160 million children, by providing proof of age (White & Madgavkar, 2019).

This research work is a comparison study of European Initiatives with the Indian initiative in digital identity use cases. The aim of this research is to propose an effective implementation strategy to diffuse the wide range of digital identity use cases in developing countries. This

study also focuses on understanding how developing countries can adjust their digitalization strategy in diffusing this technology.

1.2. Motivation for this research

There are several potential motivations for this research on the absence of a common/standard login for both public and private self-service solutions in India, including:

Improving Access to Services: Digitalization can improve access to services for citizens, but the lack of a common/standard login solution may limit the potential benefits. By exploring the barriers to adoption and potential solutions, this research can help improve access to services for citizens in India. A national digital identity solution can make it easier for citizens to access online services. It can reduce the need for physical documents and reduce the time required to access services. For example, in Estonia, citizens can access over 3,000 services online using their digital identity(European Union, 2016).

Addressing Security Concerns: A national digital identity solution can enhance security and reduce the risk of identity theft and fraud. By understanding the potential barriers to adoption and developing effective strategies for adoption, this research can help address security concerns and improve the overall digital ecosystem in India. The World Bank reports that identity theft costs the global economy over $200 billion each year. A national digital identity solution can help reduce this cost by increasing the security of online services (World bank, 2019).

Boosting Economic Growth: The adoption of a common/standard login solution can help boost economic growth by improving the efficiency of digital transactions and increasing financial inclusion. By developing effective strategies for adoption, this research can help boost economic growth and development in India.

Enhancing Digital Governance: The development and implementation of a national digital identity solution can enhance digital governance in India. By exploring the current state of

development in national digital identity in both the EU and India, this research can provide insights into how digital governance can be improved in India.

This research can have significant implications for improving access to services, addressing security concerns, boosting economic growth, and enhancing digital governance in India. These potential benefits can be a good motivation for this research.

1.3. Drivers and stakeholders

The use of digital identity solutions is becoming increasingly important in many countries as more services move online. A national digital identity solution can provide secure and convenient identification and authentication services to citizens, businesses, and government agencies. In this essay, we will discuss the drivers and stakeholders involved in national digital identity solutions.

Drivers involved in the national digital identity solutions -

Digital Transformation: The need to digitize services and processes is a key driver for national digital identity solutions. As more services and transactions move online, there is a need for reliable and secure digital identification and authentication solutions to ensure that individuals and businesses can access services easily and safely (European Commision, 2020).

Increased Security Concerns: With the increase in cybercrime and identity theft, the need for secure and reliable digital identity solutions have become more apparent. A national digital identity solution can help mitigate these risks by providing a secure means of identification and authentication for individuals and businesses (World bank, 2019).

Economic Benefits: A national digital identity solution can bring significant economic benefits to a country. For example, it can reduce fraud, increase efficiency, and lower the costs associated with identity verification processes.

Stakeholders Involved in National Digital Identity Solutions -

Government: Governments are often the driving force behind national digital identity solutions. They have a key role in setting policies, regulations, and standards for digital identity systems. Governments also oversee the implementation of these systems and ensure that they meet the needs of citizens while protecting their privacy and security.

Technology Providers: Technology providers are responsible for the development and maintenance of the digital identity solution's infrastructure. They provide hardware, software, and network systems that enable secure authentication, storage, and transmission of identity data (Madon & Schoemaker, 2021).

Identity Providers: Identity providers are responsible for verifying and authenticating the identity of individuals using the digital identity solution. They may be government agencies, private companies, or non-profit organizations. Identity providers are responsible for maintaining the accuracy and reliability of identity information and protecting it from unauthorized access or use (Madon & Schoemaker, 2021).

Businesses: Businesses may rely on national digital identity solutions to verify the identities of their customers or employees. For example, banks may use digital identity solutions to verify the identity of customers opening new accounts. By reducing the risk of fraud and identity theft, businesses can protect themselves and their customers from financial loss.

Civil Society Organizations: Civil society organizations, such as consumer groups and privacy advocates, are stakeholders in national digital identity solutions because they advocate for the protection of individual rights and privacy. These groups may monitor the development and implementation of digital identity systems to ensure that they meet these standards (Madon & Schoemaker, 2021).

1.4. Research Objectives and Scope

Objective 1:

In the literature review, the current paper will define digital identities, electronic IDs, and common login solutions. Further, the research will focus on the different national eID solutions implemented in different countries in the EU and "Digital Aadhaar" in India and discuss the current state of their development.

Objective 2:

In the theoretical framework chapters, the research will present existing theories and frameworks on the adoption of new technologies and e-governance, address their limitations, critical discussion on why a particular theory is chosen over others, and relate the parameters of the theory with the element of this research work.

Objective 3:

Analyze and assess the potential adoption of national digital identity solutions in India by using the learnings of the eID solutions in the EU and already gathered empirical data. Understand how developing countries need to adjust their digitalization strategy to diffuse this technology.

1.5. Research Questions

In this research, it is important to understand the current status of digital identity solutions development in the EU and India. The first sub-question looks at the current state of electronic IDs in the EU and India. The second sub-question is about understanding the potential barriers, implementation challenges, issues, and areas of improvement in the diffusion of the common login technology solutions. In the third sub-question, the researcher will analyze the overall literature and data gathered to find out what learnings can developing countries take from the early adopters. And in the fourth sub-question researcher will analyze the literature to find out effective strategies and the framework that helps in the diffusion of national solutions for digital identity in developing countries like India.

Main Research question:

1. Despite the growth of digitalization, India does not have one common/standard login for both public and private self-service solutions. What can be an effective strategy/framework to increase the adoption of national digital identity in India?

Sub-questions:

A. What is the current state of development in National digital identity in the EU and India?
B. What are the potential barriers that prevent the diffusion of the National digital identity?
C. What learnings can India take from the early adopters in Europe?

1.6. Structure of the report

The present thesis is structured as follows. At first, the subsequent chapter to the introduction (Chapter 1) is the literature review (Chapter 2) which talks about the research done in the field. This includes an overview of digital identity, its use cases, and the current development level. This also includes an overview of electronic IDs, digital identities, current EU developments in the field, digital Aadhaar, etc. This also includes what lessons can developing countries take from the early adopter of this technology and recommendation for developing countries like India. Chapter 3 describes the theoretical framework that serves as the foundation of this research. It contains the framework for the implementation and adoption of digital identity solutions. The methodology is in chapter 5, and it explains the methods used to collect the data. Chapter 6 addresses more details on how data is related. Based on the findings, the research questions are addressed in relation to the theories and literature that provide the main base for this thesis (Chapter 7). Finally, the last chapter contains the conclusion of this study (Chapter 8).

1.7. Expected Outcomes

The comparison study of European Initiatives with the Indian initiative in digital identity use cases can lead to several expected outcomes. By analyzing the current state of digital identity in both the EU and India, this research can provide insights into how developing countries can adjust their digitalization strategy to diffuse this technology effectively. One of the expected outcomes of this study is the identification of barriers to the adoption of digital identity solutions in developing countries like India. By understanding the factors that hinder the widespread adoption of digital identity solutions, this research can propose effective implementation strategies that address these barriers. For example, one significant barrier to adoption is the lack of awareness and understanding of digital identity solutions among citizens. This research can suggest awareness campaigns and training programs to educate citizens on the benefits of digital identity solutions. Another expected outcome is the identification of potential use cases for digital identity solutions in developing countries. By analyzing the use cases in the EU and India, this research can identify the use cases that are most relevant to developing countries. For example, digital identity solutions can help enforce legal rights and eliminate child labor by providing proof of age. By identifying these use cases, this research can suggest implementation strategies that prioritize these use cases. Additionally, this study can lead to the identification of best practices in digital identity implementation in the EU and India. By analyzing the implementation strategies in these regions, this research can identify the approaches that have been successful in diffusing digital identity solutions. These best practices can be applied to developing countries to improve the effectiveness of implementation. Furthermore, this study can lead to the development of effective strategies for the diffusion of digital identity solutions in developing countries. By synthesizing the findings from the analysis of barriers, potential use cases, and best practices, this research can propose effective strategies for the implementation of digital identity solutions. These strategies can address the specific challenges faced by developing countries, such as the lack of infrastructure and limited resources. The expected outcome of this study can have significant implications for developing countries like India. By diffusing digital identity solutions effectively, citizens can benefit from improved access to services, enhanced security, and increased economic growth. The government can benefit from improved digital governance and reduced costs associated with identity verification processes.

2. Literature Review

The emergence of digital technologies and the internet has transformed the way individuals interact with each other and the world around them, leading to the creation of new forms of identity and self-presentation. In recent years, digital identity has become a critical topic of discussion, as individuals increasingly navigate their lives and relationships online, and scholars seek to understand the implications of this new digital reality. The purpose of this literature review is to provide a comprehensive overview of the current state of knowledge on national digital identity solutions, with a particular focus on examining the adoption, diffusion, and use of digital identities in the authentication. By analyzing the existing literature, this review aims to identify key themes and trends, evaluate different research methodologies and approaches, and highlight gaps in the existing research.

2.1. What is digital identity?

Digital identity refers to the way in which an individual or organization is represented and recognized in a digital environment. It is an essential component of modern digital society and is used to authenticate users, provide access to services and resources, and facilitate online interactions. Digital identities are created, managed, and used by individuals, organizations, and online platforms. The concept of digital identity includes technical aspects such as authentication mechanisms and identity management systems, as well as social aspects such as trust and control over personal data. The management and protection of digital identity is a crucial issue in today's world, and it is an area of active research and development.

Identity is a set of attributes relating to an entity/person that gives a singular and meaningful representation of it in each situation or context, for a certain purpose. Digital identity is the utilization of these attributes to enable people or entities to engage in social and economic interactions. All electronic transactions and digital relationships are enabled by three foundational pillars (Felcourt, 2022). From fig.1, the first pillar consists of enrolment and identification, the second is user authentication - usually through checking credentials issued at the identification phase and the third is user authorization. This last pillar features an exchange of consent often through digital signatures and rights management often through the exchange and/or attestation of attributes (Felcourt, 2022).

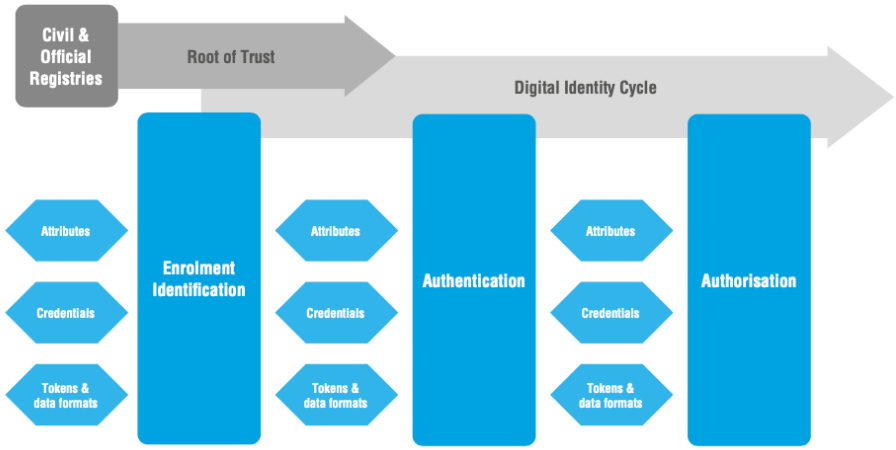

Figure 1 The three function pillars & cycle of digital identity (Source: Security identity alliance edition 2022)

Whether in the physical world or online, there are four basic reasons for using a digital identity - signing up for a new service, gaining access to a resource or personal account, making a commitment, undertaking a transaction, or signing a document and asserting rights and duties or providing something about you.

Digital identification, authentication, and authorization are related but distinct concepts. Digital identification refers to the process of establishing a unique digital identity for an individual or entity in a digital system (Felcourt, 2022). This identity can then be used to identify the user in subsequent interactions and transactions. Authentication is the process of verifying the identity of a user or device attempting to access a digital system (Puthal et al., 2019). This is typically done by requiring the user to provide some form of identification information, such as a password, a PIN, a smart card, or biometric data, which is then validated against a pre-established set of criteria (Puthal et al., 2019). Authorization is the process of granting or denying access to specific resources or services based on the authenticated user's identity and the permissions associated with that identity. Once a user has been authenticated, the digital system will determine what actions the user is allowed to perform and what resources they are allowed to access (Ezawa et al., 2023).

2.2. Electronic Identification (eID)

Electronic identification (eID) is a digital authentication system that enables individuals to prove their identity online. It is a way for people to securely and conveniently access a variety

of services and applications in the digital world, such as online banking, e-commerce, government services, and healthcare. An eID typically consists of a unique identifier, such as a username or password, along with additional security features such as biometric data or a smart card. The use of eID can help to prevent fraud, identity theft, and other security risks associated with online transactions. The concept of eID has become increasingly important in recent years, as more and more services and interactions take place in the digital world. In some countries, electronic identification is a legal requirement for accessing certain services and performing certain transactions. Electronic identification (eID) is a system that uses electronic devices to verify the identity of a person in a digital environment. The use of eID has become increasingly important in the digital age, as more and more services move online. It allows individuals to securely access digital services, make online transactions, and sign legal documents electronically, among other things. eID systems vary in their implementation, but typically involve the use of biometric data, such as fingerprints or facial recognition, as well as smart cards or mobile devices (Liu, Guo, & Yang, 2020).

One major benefit of eID is that it can reduce the risk of identity theft and fraud, as it is more difficult to fake an electronic identity than a physical one. Additionally, eID can make accessing digital services more convenient and efficient, as users can authenticate themselves without the need for physical tokens or passwords (Liu et al., 2020). However, the use of eID also raises concerns about privacy and data security, as personal information is often collected and stored as part of the authentication process. The most important framework is the electronic Identification, Authentication, and Trust Services regulation, or eIDAS, which has been fully in force since 2018. The aim of eIDAS is to strengthen trust in electronic transactions between companies, citizens, and authorities by creating a common legal framework for cross-border recognition of national electronic identification schemes and standard rules for trust services across the EU. For this reason, according to eIDAS, each EU member state can register eID schemes, which other EU members have to accept at a given level of assurance (Wunderlich et al., 2022). To address these concerns, many countries have implemented regulations and guidelines for eID systems. For example, the European Union's eIDAS regulation establishes standards for electronic identification and trust services, including requirements for data protection and security (Regulation (EU) No 910/2014, 2014). Similarly, the United States

National Institute of Standards and Technology (NIST) has developed guidelines for eID systems that emphasize privacy and security (NIST, 2017).

An E-ID allows trusted parties to identify and authenticate individuals before providing a trust service. Trusted E-IDs are thus necessary components for the implementation of electronic business processes (Andermatt & Göldi, 2018). Considering countries' experience of introducing electronic government, it has been realized that for the success of such large-scale systems, the mere implementation of a technologically elegant solution is not sufficient. The importance of end-user acceptance cannot be overlooked (Tsap et al., 2019). The deployment of eID solutions varies across Europe. It is safe to say that across Europe, all countries not only are at different stages of maturity with regard to deployment but also lack a common set of implementation mechanisms (Arora, 2008). There are different underlying motivations and implementation strategies across each country.

2.3. National Digital Identity solutions (NDI)

National Digital Identity (NDI) solutions refer to a government-led initiative to create a digital identity for its citizens, which can be used for authentication and access to various government and private services. According to the World Bank, NDI Solutions are "a foundational element of a modern digital economy and digital government," and can "improve efficiency, security, and transparency of public services while empowering citizens to exercise their rights and engage with the state (World bank, 2019)." A national digital identity solution is a system that provides a secure and reliable means of verifying a person's identity online. It is designed to enable access to digital services and transactions, including e-commerce, e-government, and financial services. National digital identity solutions are typically based on electronic ID (eID) cards, which contain personal information, such as name, address, and date of birth, as well as biometric data, such as fingerprints or facial recognition. These systems use a combination of cryptography and authentication mechanisms to ensure the privacy and security of user data. For example, Estonia's national digital identity system, called e-Estonia, is one of the most advanced in the world. It enables citizens to access a wide range of government services online, including voting, taxes, and healthcare. The system uses a combination of smart ID cards, digital signatures, and two-factor authentication to verify user identity and protect user data (Miguel, 2019).

The European Union (EU) has been at the forefront of developing and implementing national digital identity solutions. In 2014, the eIDAS (Electronic Identification, Authentication and Trust Services) Regulation was adopted by the EU to enable cross-border recognition and acceptance of electronic identities and trust services. The eIDAS Regulation aims to establish a common framework for digital identities across EU member states, enabling citizens and businesses to access services and conduct transactions online, regardless of where they are located. As a result, several EU member states have developed national digital identity solutions that comply with the eIDAS Regulation (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, 2014).

Figure 2 shows the market segment based on the level of user acceptance and maturity of technology in EU states and pioneer countries are Norway, Finland, Sweden, Denmark, and Estonia. Characteristic of these countries is the widespread use of eIDs, for example, MitID in Denmark and bankID in Norway. The acceptance and adoption of eIDs in the population in all countries of this first cluster is very high, as they are regularly used for all types of services that require identification, especially in the financial and public service area. So far, Denmark, Estonia, and Sweden have eIDs with a “notified” status, while Norway's solution has been “peer-reviewed” (Wunderlich et al., 2022).

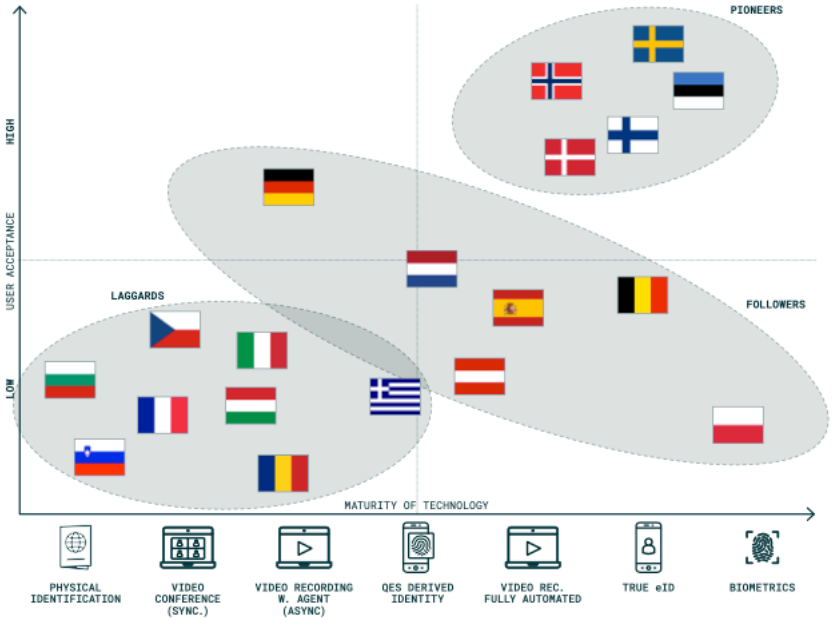

Figure 2 Market segments based on level of user acceptance and maturity of a technology. (Source: Arkwright Industry report, June 2022)

In India, the NDI solution is known as Aadhaar, which is a biometric-based identification system that assigns a unique 12-digit number to every resident of India. Aadhaar was launched in 2009 and has since become one of the largest national digital identity systems in the world (UIDAI, 2022). The Aadhaar system uses biometric data such as fingerprints and iris scans to create a unique digital identity for each resident. It also includes demographic data such as name, date of birth, and address. The Aadhaar system is intended to provide a secure and convenient way for residents to access government services and benefits, such as opening bank accounts and applying for passports (The Aadhaar Act, 2016). Since its launch, Aadhaar has faced criticism from privacy advocates who argue that the system poses a risk to personal privacy and security. In 2018, the Indian Supreme Court ruled that Aadhaar is constitutionally valid, but limited its use to certain government services (Pranav, 2018). Aadhaar represents an important example of a national digital identity system in a developing country context. While it has faced criticisms and challenges, Aadhaar has also provided a way for millions of Indians to access government services and participate in the digital economy.

2.3.1. The current state of development of NDI solutions in the EU

Over the past decade, Europe has seen a growing interest in digital identity solutions, with many countries investing in the development of national digital identity systems. One of the most advanced systems is Estonia's e-Estonia system, which has been in place since 2002 and allows Estonians to access government services and sign documents digitally using a smart ID card (Miguel, 2019). In 2021, the Danish government launched a new digital identity solution, called "MitID," to replace NemID. MitID is based on similar technology and features two-factor authentication using a password and a physical token, but also includes additional security features such as biometric identification, which allows users to use facial recognition or fingerprint scanning to access their accounts (Mogensen, 2021). Denmark's experience with national digital identity solutions, such as NemID and MitID, has been largely positive, with high levels of user adoption and satisfaction. The system has provided a secure and reliable way for citizens and businesses to access online services and has helped to promote digital inclusion and streamline government services. BankID is a digital identification solution widely used in Sweden that enables users to identify themselves electronically and sign documents online. It is based on a two-factor authentication system, which requires users to provide both a password and a unique code generated by a physical token, such as a card reader or mobile app. BankID has been developed jointly by the major banks in Sweden, and is considered a highly secure and reliable form of digital identification (Göransson, 2018). Its technical features, such as the use of public-key cryptography and support for mobile devices, have helped to ensure the security and accessibility of online services, and have enabled the development of a digital economy in the region.

2.3.2. eIDAS (Electronic Identification, Authentication and Trust Services)

One of the most significant recent developments in the field of NDI in Europe has been the launch of the European Commission's eIDAS (Electronic Identification, Authentication and Trust Services) regulation in 2018. This regulation aims to establish a common framework for NDI solutions across the European Union (EU), with the goal of promoting interoperability and cross-border use. Under eIDAS, national NDI solutions are required to meet certain technical standards and to be mutually recognized across the EU (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, 2014).

There have been several initiatives aimed at developing pan-European NDI solutions. One of the most significant of these is the European Digital Identity Wallet, which was launched by the European Commission in June 2021. The wallet is intended to provide a single, secure platform for storing and sharing digital identities across the EU and the pilot project is expected to be rolled out in the first half of 2023 (Podgorelec et al., 2022). The wallet will allow users to store their NDI credentials, such as national identity cards, and to use them to access online services across the EU. The wallet is based on a decentralized model, which means that users retain control over their own data and can choose when and how to share it with third parties. This is in contrast to traditional centralized models, where data is stored on a central server and controlled by a single entity. Decentralized models are seen as more secure and privacy-preserving, as they reduce the risk of data breaches and give users more control over their own data (Podgorelec et al., 2022). One of the key features of the wallet is its interoperability with different national digital identity solutions across the EU. The wallet will be able to recognize and use credentials from different national solutions, making it easier for users to access online services across borders. This interoperability is facilitated by the European Commission's eIDAS (Electronic Identification, Authentication and Trust Services) regulation, which establishes a common framework for digital identity solutions across the EU (Podgorelec et al., 2022).

2.3.3. Decentralization of Digital Identities

Decentralization is becoming an increasingly important aspect of digital identity in Europe, as citizens seek greater control over their personal information and the way it is used by businesses and governments. Decentralization refers to the idea that identity data should be owned and controlled by the individual, rather than by centralized authorities or third-party intermediaries. One of the main drivers of decentralization in digital identity in Europe is the European Union's General Data Protection Regulation (GDPR), which has strengthened data protection rules and given individuals more control over their personal data. The GDPR has made it clear that

individuals have the right to own and control their personal data, and that they must give explicit consent for any processing of that data (Goodell & Aste, 2019). Some of the initiatives discussed above like ESSIF, IRMA, and Sovrin foundation are based on the decentralization of identity architecture. Decentralization in digital identity is still in its early stages in Europe, and there are challenges to be overcome, including the need for standardization and interoperability across different decentralized identity frameworks, the need to address legal and regulatory issues around data privacy and protection, and the need to ensure that decentralized identity solutions are accessible and user-friendly for all citizens (Goodell & Aste, 2019).

Self-sovereign identity (SSI) is a decentralized digital identity framework that puts users in control of their own identity data, allowing them to securely and privately manage their personal information. In Europe, there has been growing interest in SSI as a potential solution to the challenges of digital identity, including privacy, security, and interoperability. One of the key drivers of SSI in Europe has been the European Commission's efforts to establish a single market for digital services, including digital identity. The Commission's 2018 Recommendation on the establishment of a European Electronic Identity Framework (eIDAS) called for the development of a "user-centric, privacy-preserving, secure and highly interoperable" digital identity framework that could be used across the EU (Preukschat & Reed, 2021). Since then, a number of SSI initiatives have emerged in Europe, including the European Self-Sovereign Identity Framework (ESSIF) project, which is funded by the European Union's Horizon 2020 research and innovation programme. ESSIF aims to establish a framework for interoperable and privacy-preserving digital identities that can be used across different sectors and domains, including e-government, e-commerce, and financial services (Preukschat & Reed, 2021). SSI is a promising framework for digital identity in Europe, with the potential to address many of the challenges associated with centralized and siloed digital identity solutions. The European Commission's support for SSI, as well as initiatives such as ESSIF, the Sovrin Foundation, and IRMA (I Reveal My Attributes), are helping to advance the development of decentralized, user-centric digital identity solutions in Europe. However, there are still challenges to be overcome, and continued collaboration and innovation will be needed to realize the full potential of SSI in Europe.

2.3.4. Privacy Laws, Regulations, and Frameworks

Different countries, like the United States and the European Union, passed laws to address the gap in regulations. They have all been segregated initiatives to try to protect digital information and identities. With the emergence of these rules and regulations, people lack the awareness of what these rules do and what kind of risks they help protect them against (Sullivan, 2018). One recently published law that had a significant impact internationally on digital personal information is the enforcement of the General Data Protection Regulation in the European Union (European Union, 2016). The National Institute of Standards and Technology (NIST) put together a framework, NIST 800-63-3, explaining digital identity and its attributes. In essence, the framework was 12 geared towards enterprises and United States government agencies, to be used as a guideline to manage digital identity and authentication mechanisms. This framework defines digital identity as well as its attributes and minimum technological use standards (NIST, 2017).

2.4. Aadhaar: India's Initiative in national digital identity solution

A crucial factor that determines an individual's well-being in a country is whether their identity is recognized in the eyes of the government. Weak identity limits the power of the country's residents when it comes to claiming basic political and economic rights. The lack of identity is especially detrimental for the poor and the underprivileged, the people who live in India's "social, political and economic periphery". Agencies in both the public and private sectors in India usually require clear proof of identity to provide services. Since the poor often lack such documentation, they face enormous barriers in accessing benefits and subsidies (Sao, 2013). Aadhaar, India's program to provide a unique identification number for every resident, is the largest biometric identification program in the world. The program also aims to achieve social inclusion and more efficient public and private service delivery. Aadhaar has also started to be used for several public purposes, such as digitizing government subsidy flows (G2P [government-to-person] payments); financial services; recording attendance for government employees to reduce absenteeism; and issuance of passports, voter identity cards, and other forms of ID (Banerjee, 2016). Many Indian residents today have several forms of identity for different purposes, such as a voter ID card, a ration card for accessing the public distribution

system, a Permanent Account Number (PAN) card for tax registration, a driver's license, and a passport. The application and verification process for each of these IDs is different and procedurally complex. The government proposed creating a single biometric identification system that would be housed in and monitored by the Unique Identification Authority of India (UIDAI) and that would allow a more accurate picture of Indian residents and their access to and use of public services (Banerjee, 2016). On January 28, 2009, the UIDAI was constituted as an attached office under the aegis of the Planning Commission and was entrusted with issuing the Aadhaar numbers and maintaining the demographic and biometric database of the residents (Sao, 2013).

UIDAI provides an authentication facility for verifying the identity information of an Aadhaar number holder through the process of authentication, by providing a Yes/ No response or e-KYC data. Modes of Authentication -

- Demographic Authentication
- One Time Pin based Authentication.
- Biometric-based Authentication (Fingerprint, Iris, and Facial Image)
- Multi-factor Authentication (UIDAI, 2022)

Fig. 3 shows the Aadhaar authentication transactions by different modes/agencies. According to the Unique Identification Authority of India (UIDAI), the agency responsible for issuing Aadhaar numbers, there were over 3.41 billion Aadhaar authentication transactions conducted in India between January and November 2021 alone.

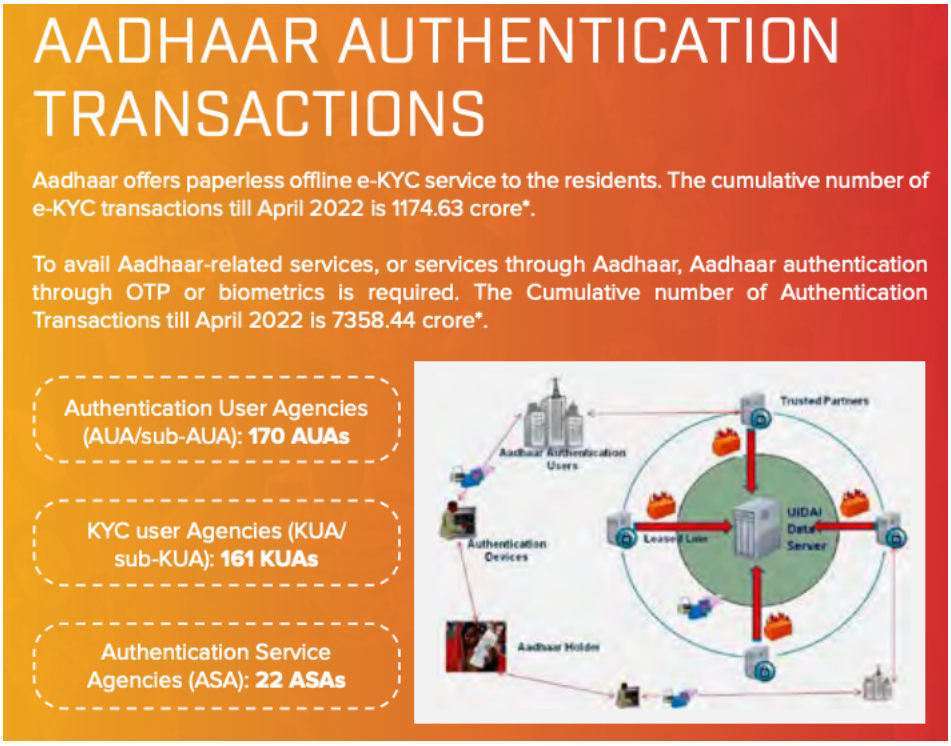

Figure 3 Aadhaar authentication transactions Source: (UIDAI, 2022)

Data from the UIDAI (Fig. 4) shows that the number of overall Aadhaar authentications is growing steadily. Similarly, the number of unique IDs (UIDs) authenticated continues to trend upward (UIDAI 2018). In February 2018, 271 million individuals used their Aadhaar to authenticate themselves, representing nearly one in four people in possession of an Aadhaar (Abraham et al., 2018).

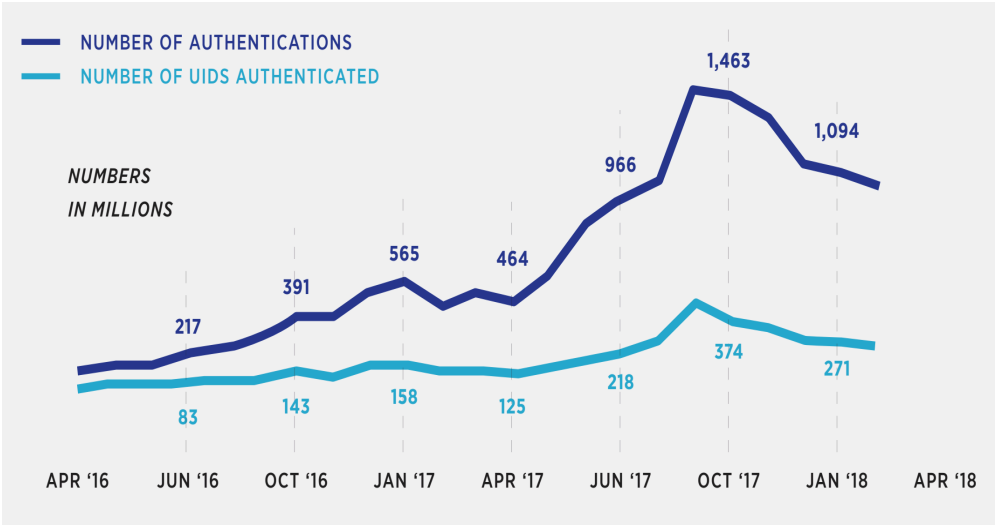

Figure 4 Aadhaar authentication and unique residents authenticated over time, Apr 2016 – Feb 2018 (Source: UIDAI Dashboard)

2.5. Potential barriers that prevent the adoption of national digital identity

While national digital identity (NDI) solutions have the potential to bring many benefits, there are also potential barriers that can prevent their adoption. Addressing these barriers will require a concerted effort from governments, industry, and civil society to ensure that NDI solutions are secure, trustworthy, and accessible to all.

Lack of trust - "Trust" is displayed as a two-type concept that included institution-based trust and characteristic-based trust. The institution-based trust represents the trust that citizens experience towards public authorities and their activities, whereas characteristic-based trust is the one that end users put in the system or solution (Tsap et al., 2019). Another study (Brunel University & McGrath, 2016) identifies 'trust' as well as 'distrust' as two independent and separate sides of the same relationship and not as two opposites of one continuum. These two sides, as the authors explain, co-exist and evolve as the relationship matures and evolves over time. Here, the term 'relationship' is used in the socio-technical and political context. Therefore, ambivalence is the main attribute and finding regarding trust and distrust that variates from country to country clearly influencing the development outcomes.

Technical challenges - Implementing a national digital identity system can be technically complex, and there may be challenges in integrating it with existing systems or ensuring that it is interoperable with other countries systems. One of the biggest challenges is to ensure that different digital identity systems across the EU are interoperable. This requires the establishment of common standards and protocols that enable different systems to communicate and exchange data (Podgorelec et al., 2022). With the right approach and technology, a national digital identity system can provide citizens with a secure and convenient means of accessing digital services, while promoting trust and efficiency in the digital economy.

Awareness - Some people may be unaware of the benefits of national digital identity systems, or may not understand how they work, which could make it difficult to get them to adopt the system (Tsap et al., 2019). With the emergence of rules and regulations related to security and privacy, people lack the awareness of what these rules do and what kind of risks they help protect them against (Sullivan, 2018).

Cultural and historical factors - Various cultural and historical elements play a role in the evolution of e-ID systems in countries. For example, in countries with a history of national ID cards and the use of central population registers, the population may be more accepting of e-ID systems that extend on existing functionality. Moreover, the organizational structure may also be in place to deploy an e-ID system, which may make deployment easier. For example, prior to the rollout of its e-ID system, Belgium had developed a robust identity infrastructure including a national register, personal identifiers, and a national ID card. Belgium already had a compulsory national ID system in place before its e-ID was developed, and had issued ID cards since 1919 (Castro, 2011). One cultural factor that has influenced the development of eID and digital identity is the level of trust that individuals have in their government and other institutions. For example, in countries where there is a high level of trust in the government, such as Sweden and Estonia, eID has been widely adopted and is used for a variety of purposes, including voting and accessing healthcare services. Conversely, in countries where there is a lower level of trust in the government, such as Greece and Italy, eID adoption has been slower (Miguel, 2019). Countries with a high level of technological advancement, such as Sweden, Estonia & Denmark, have been able to develop sophisticated eID and digital identity systems that are widely adopted and integrated into various aspects of daily life. In contrast, countries with lower levels of technological advancement, such as many African countries, face significant challenges in developing and implementing eID and digital identity systems(World bank, 2019).

Organizational Issues - Various aspects of e-ID systems are implemented at either the national or local level. Some components may be more efficient to implement and manage at the national level, while others may be better left to local government. Various countries approach this issue differently. For example, Denmark's e-government strategy is to allow the implementation of solutions at the local level while using common standards and frameworks where necessary to simplify legal, organizational, and technical issues (DIGST.dk, 2021).

Privacy concerns - Privacy concerns are common with many applications of technology, especially those that involve personally identifiable information. Some privacy advocacy groups oppose all efforts to build an e-ID system regardless of how well the system is designed.

These groups fundamentally object to the government collecting and processing personal information and view this as an unjust intrusion of government into an individual's right to privacy. When it comes to eID and digital identity, privacy concerns are a major factor that affects their adoption and usage. Digital identities can contain a wealth of personal information, ranging from name and address to biometric data, and this can lead to privacy risks if not managed properly. For instance, unauthorized access to digital identity information can result in identity theft or other types of fraud, and this can have serious consequences for individuals and businesses (Mooij, 2023).

Financial Investment - Rolling out e-ID solution is not only complex but also bears significant financial burden on country and up to some extent on the citizens. This is also one reason why some countries do not want to start this kind of project and would rather prefer the security provided by PIN or Password. The electronic identification system using smart cards involve smart cards itself which consists of the plastic body and a microprocessor, the physical security features related to the card, card readers, relevant documentation, developing specific applications, distribution system, a registration authority, PKI, Cross-certification, Time stamping, and Client-side software interacting in a consistent, trustworthy manner. Establishing this infrastructure needs substantial investment. The financial investment required for eID and digital identity systems can still be a significant barrier to adoption for some organizations and governments. To address this issue, governments and other stakeholders can explore alternative funding models, such as public-private partnerships or user fees, to help offset the costs of implementing these systems (Kő et al., 2019).

2.6. Lessons from Early adopters of National Digital Identity solution

Legal framework for electronic IDs - A legal framework is a prerequisite for the widespread use of e-IDs to create legally-binding signatures. Such a framework is necessary as the use of electronic signatures can only prosper if they are recognized as valid legal mechanisms. Legislation creating the legal regime for electronic signatures must balance both security and efficiency. As policymakers increase the strictness of technical standards, they may improve the security of electronic signatures, but decrease technology neutrality and discourage innovation (Castro, 2011).

Cultural and Historical factors - Judging from the list of successfully deployed national digital identity solutions, it is evident that the leaders are predominantly countries like Denmark with smaller populations. In addition, these countries generally embrace information technology, have above-average broadband rankings, and have forward-thinking e-government strategies. Arguably, a small country may be more nimble in its policymaking. For example, a small country with a homogenous population may not face the same political resistance when proposing new technology projects that would be found in a more politically divided nation. However, small countries are not necessarily at an advantage. Their IT systems generally have higher fixed costs and lower marginal costs. Thus, large countries like India should expect to be able to build a national digital ID system at a lower average cost per user than smaller countries (World bank, 2019).

Policy issues - Issuing e-IDs to citizens and residents is only one step towards creating a robust national system for electronic identity management. Many nations have also adopted demand-side policies to spur faster adoption and more use of e-IDs. For the most part, this has meant investment in e-government initiatives that use e-IDs to make interacting with the government more citizen-friendly and efficient as filing taxes, obtaining government benefits, signing government documents, making payments, and paying for public transportation. Many countries also have programs to broadly increase the adoption and use of digital technology (European Commission, 2019).

Technology issues – Most of the efforts at establishing interoperable e-ID systems have occurred between EU member states. eIDAS (Electronic IDentification, Authentication and trust Services) is a European Union regulation that establishes a framework for electronic identification and trust services for electronic transactions in the European Single Market. One aspect of eIDAS is interoperability, which refers to the ability of different eIDAS-compliant systems to work together seamlessly. This means that an eIDAS-compliant digital identity system in one EU member state should be able to be used to access services in another member state, without the need for additional authentication. These efforts require that nations establish both technical and legal measures to ensure cross-border interoperability (Tsakalakis et al., 2019). Still, technical interoperability between various e-ID solutions is fairly minimal and

users face interoperability challenges. Some countries face interoperability problems even within the country.

Privacy – Privacy advocates raise objections to the use of enhanced identification cards or national identification cards, citing potential threats to civil liberties, including increased monitoring and surveillance and a decrease in anonymous free speech. Certainly, some of these objections are valid: totalitarian governments can and have used this type of technology to decrease personal freedom. However, technology does not dictate the values of society. While totalitarian governments may have created national IDs, national IDs did not create totalitarian governments. As the experience of many countries has shown, free and democratic societies use national ID cards to make government more efficient and productive. Taken as a whole, the benefits of using technology to improve ID systems vastly outweigh the risks. Still privacy concerns have derailed some efforts at deploying e-ID solutions. For example, in Denmark the Ministry of Finance, Ministry of Interior and the Local Government Denmark (an association of Danish municipalities) tried to create a single, multi-purpose e-ID card in the 1992 to replace the existing array of ID solutions (such as the driver's license and SIS-card), but their efforts were stalled by privacy concerns raised by policymakers in Parliament (Mooij, 2023).

2.7. Summary

There are a number of obstacles that can hinder the adoption of national digital identity solutions. Implementing a national digital identity solution can be expensive, as it requires the development of new systems and infrastructure, as well as ongoing maintenance and support. This can be a barrier for countries with limited financial resources. In order to use a national digital identity solution, individuals need to have access to technology such as computers, smartphones, or biometric scanners. If a country lacks the necessary technical infrastructure, it can be difficult to implement and adopt a national digital identity solution. Some individuals may be concerned about the privacy implications of a national digital identity solution, as it involves the collection and storage of personal information. It is important for countries to have strong privacy laws and practices in place to address these concerns. Many people are accustomed to using traditional forms of identification, such as physical identity documents, and may be resistant to adopting a new digital system. It can be challenging to convince

individuals to switch to a digital identity system, especially if they are not familiar with technology or are skeptical of its benefits. Implementing a national digital identity solution can involve a complex array of legal and regulatory issues, such as data protection laws, intellectual property rights, and cybersecurity. It can be difficult to navigate these issues and ensure that a national digital identity solution is compliant with relevant laws and regulations.

There are a few recommendations that early adopters of national digital identity solutions might make to countries considering the implementation of such a system. It is important to involve a diverse group of stakeholders, including government agencies, private companies, civil society organizations, and individual citizens, in the planning and implementation of a national digital identity solution. This can help to ensure that the solution meets the needs of all parties and addresses any concerns that they may have. A national digital identity solution should be easy for individuals to use and understand. This can involve designing user-friendly interfaces, providing clear instructions, and offering customer support to help users with any issues they encounter. National digital identity solutions involve the collection and storage of sensitive personal information, so it is important to have strong security measures in place to protect this data. This can include measures such as encryption, secure servers, and regular security audits. It is also important to have clear privacy policies in place and to ensure that individuals are aware of how their personal information will be used. It can be helpful to provide education and outreach to individuals and organizations about the benefits and uses of a national digital identity solution. This can help to build awareness and understanding of the system and encourage adoption. It is important to continuously monitor and evaluate a national digital identity solution to ensure that it is meeting its intended goals and to identify any areas for improvement. This can involve collecting feedback from users and analyzing data on usage and performance.

3. Theoretical Background

The theoretical background chapter is crucial for establishing the intellectual framework and theoretical context for the research. This chapter provides a comprehensive overview of the existing theories and concepts that inform digital identity research, including concepts such as identity, privacy, security, and trust. It helps to identify gaps in the existing literature and establish the research questions or problems that the study seeks to address. It informs the research design and methodology by providing a foundation for selecting appropriate research methods and data collection techniques.

The theories like stakeholder theory, diffusion of innovation, and technology acceptance model are options available that could have been used in this study. But Comparative institutional analysis theory is chosen over others because it is more suitable for this study as elaborated subsequently. **Stakeholder theory** is a management and business theory that proposes that businesses should consider the interests and needs of all stakeholders, not just shareholders when making decisions. Stakeholders include employees, customers, suppliers, local communities, and society at large. The theory suggests that a company's success should be measured not just by financial performance, but also by its ability to create value for all stakeholders (Freeman et al., 2010). Stakeholder theory was developed primarily for business contexts and may not be as relevant for understanding digital identity adoption, which involves a broader range of actors and social dynamics. There is a lack of specificity as Stakeholder theory provides a broad framework for understanding the relationships between businesses and their stakeholders, but it does not offer specific guidance for conducting research on digital identity adoption. **Diffusion of innovation** theory focuses on how new ideas, technologies, and practices spread through a society, and how different factors such as the characteristics of the innovation, the adopter, and the social system affect the rate and extent of adoption (Rogers, 1983). It provides a useful framework for understanding the process of adoption of national digital identity solutions, but it does not necessarily provide a detailed understanding of the institutional factors that shape the development and implementation of these solutions. The **Technology Acceptance Model** (TAM) is a well-known theory in the field of information systems and technology that explains how users adopt and use new technologies. TAM proposes that perceived usefulness and perceived ease of use are key factors that influence an

individual's intention to use technology and their actual usage behavior (Marangunić & Granić, 2015). TAM focuses on the individual-level factors that influence technology adoption and usage and does not consider the social and contextual factors that shape digital identities. The digital world is complex and constantly evolving, and individuals' digital identities are shaped by their social interactions and the social norms and expectations associated with their online communities (boyd, 2014).

3.1. Comparative Institutional Analysis

Comparative institutional analysis theory focuses on how institutions such as laws, regulations, and norms shape behavior and interactions in a society, and how different institutional arrangements can affect economic, social, and political outcomes. This approach provides a more detailed and nuanced understanding of the institutional factors that drive the development and implementation of national digital identity solutions, including the legal and regulatory frameworks, technical infrastructure, stakeholder engagement, and cultural and social factors (Kaneriya & Patel, 2020). While the diffusion of innovation theory has its uses, I would argue that comparative institutional analysis is a more appropriate framework for research about national digital identity solutions, as it provides a more comprehensive understanding of the institutional factors that shape the development and implementation of these solutions.

Comparative institutional analysis is an approach used in social sciences, particularly in economics, political science, and sociology, to compare and contrast different institutional arrangements or systems in different countries or regions. In this approach, institutions are defined as formal and informal rules, norms, and practices that shape human behavior and interactions in a given society (Casper & Whitley, 2004). The analysis aims to identify the similarities and differences in the functioning of institutions across different societies and to understand how these institutional arrangements affect economic, social, and political outcomes. Comparative institutional analysis often involves examining the historical, cultural, and political context of different societies and the ways in which institutions are shaped and influenced by these factors. It can help to explain why certain institutional arrangements are more successful in achieving specific outcomes in one society but not in others. Comparative institutional analysis can certainly be used to compare technology between two different countries. Technology is often seen as an important factor that drives economic growth and

development, and it is shaped by institutional arrangements in each country (Kornelakis & Hublart, 2022).

While there is a growing body of literature on digital identity and its implementation in different countries, there is still a lack of research that compares the institutional factors that shape the development and implementation of digital identity solutions in different contexts. Comparative institutional analysis theory can help to address this gap in the literature by providing a framework for comparing and contrasting the institutional arrangements that shape digital identity solutions in the EU and India. For example, comparative institutional analysis theory can help to identify the ways in which government policies, regulatory frameworks, technical infrastructure, stakeholder engagement, and cultural and social factors interact to shape the development and implementation of digital identity solutions in the EU and India. It can also help to explain why certain institutional arrangements are more successful in achieving specific outcomes in one context but not in the other (Casper & Whitley, 2004).

A comparative institutional analysis can identify the **similarities and differences** in the institutional factors that shape digital identity solutions in the EU and India. Both regions may have similar goals for digital identity, but the institutional arrangements for achieving those goals may differ. It can help to identify how **government policies and regulations** in the EU and India shape digital identity solutions. Different approaches to privacy protection and data governance can influence the design and implementation of digital identity systems in these regions (Kaneriya & Patel, 2020). **Cultural factors** can also shape digital identity solutions, and comparative institutional analysis can examine the **cultural attitudes toward risk-taking** in the EU and India. If there is a greater willingness to take risks in one region, this may lead to faster adoption of new digital identity solutions. **Legal and regulatory frameworks** can have a significant impact on digital identity solutions, and comparative institutional analysis can compare the frameworks in the EU and India. Differences in legal liability for data breaches can affect the design and implementation of digital identity systems (Kaneriya & Patel, 2020). Comparative institutional analysis can provide valuable insights into the institutional factors that shape digital identity solutions in the EU and India and help to identify areas where improvements can be made to enhance the success of these solutions. By adopting a comparative institutional analysis, the research can provide valuable insights for policymakers,

academics, and other stakeholders to improve digital identity management in both regions (Kaneriya & Patel, 2020).

3.2. Christopher Allen's Principles of Self-Sovereign Identity

Christopher Allen's ten principles are a key element in this research as they can provide a framework for evaluating the effectiveness and security of digital identity systems. These principles focus on the importance of user control, privacy, security, and interoperability, among other factors. By using these principles as a guide, this research analyzes and compares different digital identity solutions and identifies areas for improvement. Additionally, the principles can help ensure that digital identity systems are designed with the user in mind, rather than solely for the benefit of government or commercial entities. Christopher Allen's ten principles can help to ensure that national digital identity solutions are effective, secure, and user-centric.

Christopher Allen's 10 Principles are the following:

1. *Existence: Users must have an independent existence.*
2. *Control: Users must control their identities.*
3. *Access: Users must have access to their own data.*
4. *Transparency: Systems and algorithms must be transparent.*
5. *Persistence: Identities must be long-lived.*
6. *Portability: Information and services about identity must be transportable.*
7. *Interoperability: Identities should be as widely usable as possible.*
8. *Consent: Users must agree to the use of their identity.*
9. *Minimalization: Disclosure of claims must be minimized.*
10. *Protection: The rights of users must be protected* (Allen, 2016).

In Europe, the concept of individual sovereignty is fundamental to digital identity. The European Union recognizes the importance of individuals having control over their personal data and the right to exist independently of any centralized authority or service provider. The European Digital Identity Framework proposes a decentralized identity model, where individuals can create and control their digital identities independently of any central authority (Stefan, 2020). The principle of control is closely related to the concept of individual

sovereignty. The European Digital Identity Framework emphasizes the importance of individuals having control over their data and being able to choose which attributes they share with third parties. The framework proposes the use of verifiable credentials, which allow individuals to selectively disclose only the information required for a particular transaction (Stefan, 2020). The principle of access is crucial for ensuring transparency and trust in digital identity systems. The European Union recognizes the importance of individuals having access to their personal data and being able to verify the accuracy and completeness of that data. The European Digital Identity Framework proposes the use of advanced cryptography and blockchain technology to provide secure and transparent access to personal data (Stefan, 2020). Transparency is essential for establishing trust and accountability in digital identity systems. The European Union emphasizes the importance of transparency in all aspects of digital identity, including the collection, processing, and sharing of personal data. The European Digital Identity Framework proposes the use of open standards and protocols to ensure transparency and interoperability (Mooij, 2023). The principle of persistence emphasizes the importance of digital identities being long-lived and able to evolve over time. Decentralized identity model allows individuals to control the lifecycle of their digital identities and update them as needed. The European Union has implemented the eIDAS Regulation to facilitate cross-border identity verification and authentication. Interoperability is essential for enabling individuals to use their digital identities across different services and platforms. The eIDAS Regulation facilitates cross-border identity verification and authentication (Tsakalakis et al., 2019). The principle of consent emphasizes the importance of individuals having control over the use of their personal data. The General Data Protection Regulation (GDPR) ensures that individuals have control over the use of their personal data. The European Digital Identity Framework proposes the use of verifiable credentials and selective disclosure to ensure that individuals give consent for the use of their personal data (Stefan, 2020).

In the context of national digital identity, the principles can be used to ensure that the system is user-centric and provides individuals with control over their personal information. The principles can also help to promote trust and transparency in the system (Preukschat & Reed, 2021). The principle of "Existence" can be applied to ensure that each individual has a unique digital identity that is not linked to any other identity. This can help to prevent fraud and ensure the accuracy of the information in the system (Mogensen, 2021). The principle of "Control"

can be applied to ensure that individuals have the ability to control the use of their personal information. This can be achieved through features such as consent management and data-sharing preferences (Hayes et al., 2013). The principle of "Access" can ensure that individuals have access to their own data and can view and manage their personal information. This can be achieved through features such as self-service portals (Tsakalakis et al., 2019). The principle of "Transparency" can ensure that the system is transparent and that individuals can understand how their personal information is being used. This can be achieved through features such as privacy policies and data usage reports (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, 2014). The principle of "Persistence" can ensure that individuals have a long-term digital identity that can be used throughout their lifetime. This can help to reduce the need for individuals to create new identities for different purposes. The principle of "Portability" can be applied to ensure that individuals can move their digital identities and personal information between different systems and services (Tsakalakis et al., 2019). This can help to promote competition and innovation in the market for digital identity services. The principle of "Interoperability" can ensure that digital identities are interoperable across different systems and domains. This can help to reduce the complexity and cost of digital identity management for individuals and organizations (Kaneriya & Patel, 2020).

4. Framework for designing a National Digital identity solution for Developing countries.

Comparative institutional analysis is a method used to compare and evaluate different institutional arrangements and their effectiveness in achieving specific goals. In the case of national digital identity solutions, this method can be used to compare the institutional arrangements of different countries and identify the strengths and weaknesses of each approach. Christopher Allen's principle is a set of principles that are essential for building a trustworthy identity system. These principles can be used to evaluate the design of national digital identity solutions to ensure that they are trustworthy and secure. By combining these two methods, a framework for designing a national digital identity solution for developing countries can be developed. The comparative institutional analysis can be used to identify the institutional arrangements that are most effective in achieving the desired outcomes, while Christopher Allen's principle can be used to ensure that the identity system is trustworthy and secure.

The framework for designing a national digital identity solution for developing countries:

Comparative Institutional Analysis:
This step involves identifying the institutional arrangements used in different countries for national digital identity solutions. It also involves comparing the effectiveness of each approach in achieving desired outcomes and identifying the strengths and weaknesses of each approach. The goal of this step is to gain a better understanding of the different institutional arrangements used in various countries and to identify the most effective approach for developing a national digital identity solution.

Christopher Allen's Principle:
This step involves evaluating the design of the national digital identity solution based on Christopher Allen's principles.This step ensures that the identity system is trustworthy and secure and that users have control over their personal information.

Framework for Designing a National Digital Identity Solution for Developing Countries:

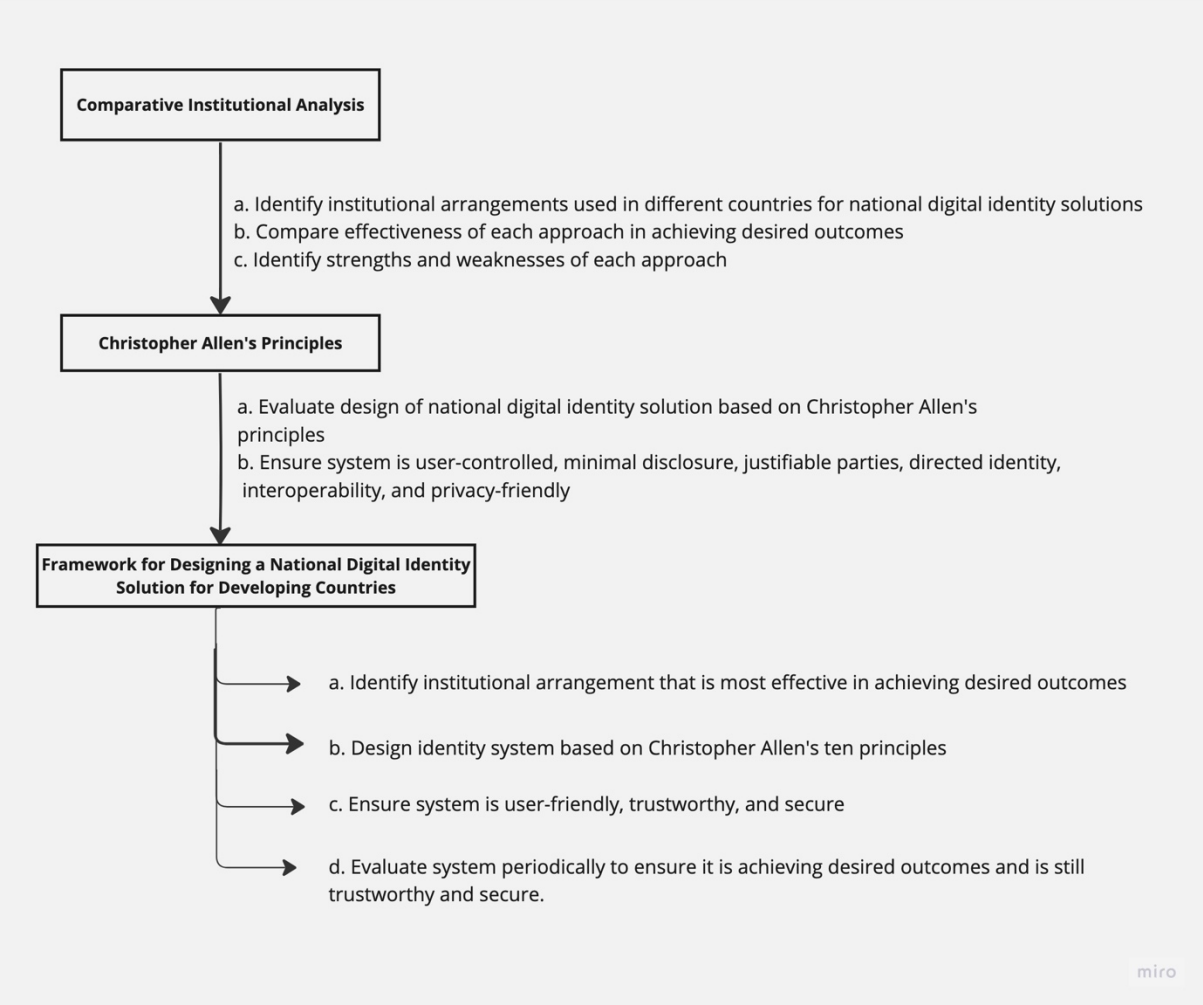

Figure 5 Framework for Designing a National Digital Identity Solution for Developing Countries

Framework for Designing a National Digital Identity Solution for Developing Countries - highlights the unique challenges that developing countries face in implementing national digital identity solutions. These challenges can include weak institutional arrangements and governance structures, a lack of infrastructure and resources, and limited privacy protections. Therefore, identifying an effective institutional arrangement and designing a system that addresses these challenges is critical to ensuring the success of the identity system.

a. Identify institutional arrangements that are most effective in achieving desired outcomes: Developing countries should identify institutional arrangements that align with their specific needs and objectives. For example, the government may take a leading role in implementing the identity system or partner with the private sector to develop the system. The institutional

arrangement should consider factors such as capacity, infrastructure, and resources available in the country.

b. Design identity system based on Christopher Allen's ten principles:
Developing countries can design their identity system based on Christopher Allen's ten principles to ensure that it is user-friendly, trustworthy, and secure. For example, the principle of minimal disclosure can be particularly important in developing countries where privacy protections may not be well established. A system that collects only the necessary information and ensures user consent can help address privacy concerns.

c. Ensure the system is user-friendly, trustworthy, and secure:
Developing countries must ensure that their identity system is user-friendly, trustworthy, and secure. To achieve this, the system should be designed with the user in mind and be easy to use. Additionally, the system should be trustworthy and secure, with proper encryption and access controls in place. Periodic evaluations and updates can help ensure the system is still achieving desired outcomes and is still trustworthy and secure. This requires a strong focus on monitoring, maintaining and updating the system regularly.

The blend of comparative institutional analysis and Christopher Allen's principles can be used in combination to design a framework for designing national digital identity solutions in developing countries. Firstly, comparative institutional analysis can be used to identify the institutional arrangements used in different countries for national digital identity solutions. This approach can help to understand the strengths and weaknesses of different approaches and identify the most effective institutional arrangement for developing a national digital identity solution in a specific country. Secondly, Christopher Allen's principles can be used to evaluate the design of the national digital identity solution to ensure that it is trustworthy and secure. This step can help to ensure that the identity system is designed with the user in mind and meets the basic requirements of privacy, security, and user control over personal information.

By combining these two methods, a framework for designing a national digital identity solution for developing countries can be developed. The institutional arrangement identified through comparative institutional analysis can be used as a basis for designing the identity system, while

Christopher Allen's principles can be used to ensure that the system is user-friendly, trustworthy, and secure. This approach can help to ensure that national digital identity solutions in developing countries are designed based on the specific needs and objectives of the country while meeting the basic requirements of trust, security, and user control over personal information. The framework can also help to address the unique challenges that developing countries face in implementing national digital identity solutions, such as weak institutional arrangements and limited resources.

5. Methodology

This chapter describes the research methodology used to fulfill the study scope. The current literature provides a general discussion about the current level of development in the EU and in India in digital identity solutions. Moreover, to analyze and answer the research question that has been formulated, more in-depth discussion is required. I planned to conduct semi-structured interviews with related experts and stakeholders for deeper understanding and analysis.

I went through several scientific search engines, and platforms to develop a literature review and theoretical framework. Google Scholar, Sci-Hub, and Libgenesis are the most notable ones. While searching, the most notable keywords that I used are, “Digital Identity”, “Diffusion”, “Electronic ID”, “Digital Inclusion”, “adoption”, “innovation”, “MitID”, “barriers”, “Digital Aadhaar”, “eIDAS, “electronic identity”, “national eID”, “obstacle”, “driver” “factor”, “determinant” “influence”, “impact”, “affect”, “user acceptance”, “public acceptance”, “citizen acceptance”, “perception”, “attitude”, “user perception”, “citizen perception”, “use”, and “usage”. I combined and matched the keywords during searching to find the relevant information.

Resources Searched - Using the keywords above, the following databases were searched:

- Google Scholar
- ACM Digital Library
- ScienceDirect
- Web of Science
- Springer Link
- IEEE Explore

To increase the number of found materials that fit the search criteria, the keywords were used in a direct search in the key journals and conference proceedings of the area. Additionally, each fitting item’s reference list was scanned through for containing possible relevant materials.

Document Selection - The document selection is based on the following inclusion and exclusion criteria: Authors include studies that: directly answer the research question;

specifically focus on eID and not just e-government; mention the issue of acceptance of digital identity by citizens; based on empirical data; specifically mention societal aspects of technology acceptance of eID.

Document Retrieval - The search has elicited 118 sources from databases. 61 of those were rejected based on the title and abstract analysis. The remaining sources were then evaluated based on the document selection criteria. The final revised list of selected papers is comprised of 57 items. Among the selected sources such types of documents were included in the review as conference proceedings, journal articles, book chapters, reports, policy documents, and theses.

5.1. Design

Making use of national digital identity to authenticate citizens in public or private sector services is quite a new technology and its value can take various facets – the research design chosen in this paper is exploratory design. In line with the research design and approach taken, this paper reviews the extant literature and uses it along with the empirical data collected from interviews for the purposes of data analysis. The research will follow a qualitative and deductive approach. The semi-structured interviews and systematic literature review maintain the qualitative method and "thematic analysis" is going to be used for the analysis. So, the questions for the interview were formulated based on the elements generated from the theoretical background by keeping in line with the literature review. As a complement to the qualitative interviews, I have used secondary sources such as official government reports and surveys performed on a nationwide scale. This design approach allowed the gathering of in-depth views and opinions of experienced practitioners involved in e-government.

5.2. Interview Questions

The formulated questions for the interview were related to the mentioned themes so that I can connect the findings properly to the research. Interview questions are categorized according to the parameters (themes) of the theories used in this research. This categorization is done based

on what does these parameters mean and possible expected answer from the interview questions.

Theme	Interview Questions
Institutional frameworks and governance structures	a) How do institutional frameworks and governance structures impact the development and adoption of digital identity solutions in different countries? b) What are the key differences in governance structures between the EU and India when it comes to digital identity, and how do these differences affect the design and implementation of national eID solutions? c) To what extent are users involved in the design and development of digital identity systems, and how does this impact trust and adoption? d) How can developing countries like India adapt existing digital identity frameworks to meet their specific needs and challenges?
Security and privacy	a) What are the key security and privacy concerns associated with digital identity systems, and how do different countries address these concerns? b) How do national eID solutions in the EU and India incorporate the principles of security and privacy by design?
Interoperability and standardization	a) To what extent are digital identity solutions interoperable and standardized across different countries and regions, and what impact does this have on cross-border e-governance and public service delivery? b) How can standardization efforts be coordinated across different countries and regions, and what challenges arise in these efforts?

	c) What are the benefits and drawbacks of using common login solutions for public and private self-service solutions, and how do different countries approach this issue?
User trust and adoption	a) How can digital identity solutions be designed to maximize user adoption and trust, and what are some of the key best practices in this area? b) To what extent do cultural factors impact user adoption of digital identity solutions, and how can these factors be taken into account in the design and implementation of national eID solutions?

Table 1 Theme based Interview questions

5.3. Data Collection

For the sake of better and more relevant analysis, I needed appropriate sources to collect data. Initially, I tried to reach the private companies in respective countries to get a basic idea of their national digital identity solution and to make them part of the research if relevant. I focused on the European countries where digital identity solution already exists and are widely used by their citizens, and also had an eye on the Nordic market as they are the pioneers in this field. By getting contacts from google search and LinkedIn I started trying to reach companies and experts by email. I had to look for some reference points to get in touch with. Then I started to read articles from Gartner & KuppigerCole and from there I got the contact information of relevant experts. I also attended digital identity-related online webinars mainly on Linkedin. To get the attention I commented by asking questions from my formulated questionnaire and asking for their contacts for further needs. Right after the session, I tried to communicate with them via email, LinkedIn, and Twitter using the webinar as a reference.

Among the 17 experts whom I have approached, 6 of them wrote me back and agreed to be part of the research. One of them is Mogens Rom Andersen who is an eID architect from Denmark. He is a Chief technical architect for MitID at the agency for digitization, therefore, fits with my research. I contacted him over LinkedIn and gave him a reference for the guest

lecture that he gave in our university class. Another expert with whom I got connected is Jens (Schødt) Schoedt from Denmark as well. He is the Director of Business Development, eSecurity Services & Digitisation at Nets Group. Working alongside Denmark's top banking experts, his team works for the e-governance services in the country. I connected with him over LinkedIn. His overall profile indicates that he was the perfect fit for my research. Another expert is from India and he is the one who set up the technology center in Bangalore which developed the Aadhaar Technology. His name is Srikanth Nadhamuni who is the Founder and CTO of Aadhaar currently working at the Unique Identification Authority of India. The fourth expert's name is Siddhartha Arora who has been working in IBM since last 27 years and has technical expertise in building digital identity solutions. He has also authored many papers about eID schemes in Europe, digital identity solutions, e-governance services, etc. The fifth expert name is Nilesh Vasita and currently he is a CTO and CEO of Trential. And the last interviewee is Siddharth Shetty who is architect at India Stack and advisor at ministry of finance, India.

I had to purchase LinkedIn Premium to send an InMail to both Indian experts as it was not possible to connect with them with regular LinkedIn. Apart from the experts, I tried to communicate with private sector companies which are helping the government to achieve its digitization goals. Among 7 such companies that I listed from Google and LinkedIn searches, 2 of the companies wrote me back and were willing to be part of the research. The first company is named "India Stack," which works on Aadhaar products such as DigiLocker, e-auth, and e-KYC (Electronic Know Your Customer) and is owned by the Unique Identification Authority of India. The second company is named "Ek Step Foundation" which is spreading awareness about the e-governance services initiatives in India.

After having potential interviewees, I had to schedule the meetings with them. The interview invitation was sent by me, and interviews were done on Microsoft Teams. I asked each of the interviewees about their consent before recording the interviews. Each interview lasted on average between 30 and 45 minutes. To schedule an interview, a notification via a phone call, SMS text message, or email was sent to each participant interviewed before each interview to arrange a date and time to meet. At the end of the interview, I informed the interviewee about the completion of the interview by saying "those were all of the questions that I wanted to ask",

and "do you have any final thoughts about National digital identity solutions that you would like to share or to add". Finally, I concluded with the following sentence: thank you for your time; I really appreciate your contribution to my study. After conducting the interviews, I had to transcript them for further analysis. "Descript" free version software was used to complete the transcription. Though the transcription was fairly on point, I still had to fix some errors in the transcript to make it more readable and understandable.

After data collection, the qualitative analysis and interpretation of the narrative data were performed with reference to the main research questions of the study and in accordance with the objectives of the study. Common themes across the challenges were identified from interview transcripts. Several important insights and themes associated with challenges were identified; those results and findings are reported in the following section of this paper.

Name	Role	Country	Interview type	Duration
Mogens Rom Andersen	Chief technical architect for MitID at the agency for digitization	Denmark	Online – Microsoft Teams	27:49
Jens (Schødt) Schoedt	Director of Business Development, eSecurity Services & Digitisation at Nets Group.	Denmark	Online – Microsoft Teams	48:03
Srikanth Nadhamuni	Founder and CTO of Aadhaar	India	Online – Microsoft Teams	35:43
Siddhartha Arora	Principal Customer Success Manager at IBM	Switzerland	Online – Microsoft Teams	47:48
Nilesh Vasita	Co-Founder & CEO at Trential	India	Online - Cisco Webex	33:40
Siddharth Shetty	Architect at India Stack, Advisor – Ministry of Finance, India.	India	Online- Cisco Webex	55:06

Table 2 Summary of Interviewees

The body language of the respondents was also observed since it helps to collect reliable information for analyzing purposes (Bell et al., 2022). Therefore, during the interviews, I tried to detect the respondent's gestures and expressions in order to test the truthfulness of their answers. During the interviews, I tried to "provoke" (in a good sense) my respondents to reflect on e-ID challenges and barriers.

The first part of the data analysis started with the process of transcribing video-recorded interviews. After all, interviews were manually transcribed, and the collected material was read several times to get a general overview of the data and to create a deeper understanding of respondent's answers.

5.4. Ethical Consideration and methodological limitations

There are several ethical aspects that I take into consideration while collecting data since I did not want my participants to feel abused or stressed. Before the interview, all participants were informed about the research purpose and that the collected data will be used only within the thesis boundary. I have also asked the respondent's permission to record the interview for an easier transcription process. Participants had no problem with me recording the entire discussion except one. In terms of methodological limitations, qualitative research is often criticized; firstly, because the results cannot be generalized (Gable, 1994) and secondly because results cannot deliver prediction (Ochieng, 2009). Moreover, due to the fact that the research study case is built around a specific country (Denmark and India), it implies that results cannot be generalized for other countries since country context and circumstances can change. However, I believe that sharing implementation experience could be beneficial to countries that are taking the first steps toward a national digital identity.

6. Findings

This section describes the findings of the empirical evidence. These findings are presented methodically by doing a thematic analysis. First, I familiarized myself with the data in the interviews. The categories based on the data were formed. The third step included finding broader themes from the thoughts of the interviewees. Here the thoughts of the interviewees are presented. This section presents the results of interviews conducted in this study. These may provide solutions to some of the challenges and obstacles that may face the successful adoption of national digital identity in developing countries. The strategy is that the interviews and the literature review will identify answers to the main and sub-research questions.
Results from the interviewees identify challenges, problems, and barriers that may need to be overcome to support successful e-Government services implementation in India. Participants were asked questions on their opinions, attitudes, and beliefs on awareness of national digital identity solutions, and the barriers which prevent the use of new technologies, such as using digital identity for authentication.

6.1. Getting Familiarized with the Data

The interviewees were diverse with their inputs on the adoption of national digital identities. The first two interviews showed a lot of areas where such solution is being used in Denmark. Many advantages were shown. The other four interviews were different and intriguing as the interviewees showed some interesting remarks about what barriers does this type of technology face in developing country like India and why does many developing countries still don't have national digital identity solutions.

6.2. Interview Codes

After analyzing the interviews the codes developed in the technical theme were- **Need for National Digital Identity, the Complexities involved, the Current state of development, Potential Barriers, the Role of E-Governance, Learning from early adopters, and Digitalization strategy.** These categories best portray the thoughts of the interviewees.

- **Need for National Digital Identity**: This theme pertains to the necessity of establishing a National Digital Identity system to enhance the efficiency, security, and transparency of digital transactions. It may include identifying the key drivers that necessitate the establishment of such a system and the potential benefits that it could offer.

- **Complexities Involved**: This theme refers to the challenges and complexities involved in designing, implementing, and maintaining a National Digital Identity system. It may include technical, operational, legal, and social complexities that need to be addressed to ensure the success of such a system.

- **Current State of Development**: This theme pertains to the current state of development of a National Digital Identity system. It may include an assessment of the progress made so far, the challenges faced, and the opportunities for improvement.

- **Potential Barriers:** This theme involves identifying potential barriers that could hinder the adoption and implementation of a National Digital Identity system. It may include factors such as lack of awareness, privacy concerns, and resistance from stakeholders.

- **Role of E-Governance:** This theme pertains to the role of e-governance in the development and implementation of a National Digital Identity system. It may include the potential benefits that e-governance could offer, such as increased efficiency, transparency, and citizen participation.

- **Learning from Early Adopters**: This theme involves studying the experiences of early adopters of National Digital Identity systems in EU. It may include identifying best practices, challenges faced, and lessons learned that could inform the development and implementation of a similar system.

- **Digitalization Strategy:** This theme refers to the overall strategy for digitalization in a country or organization. It may include the role of a National Digital Identity system within the broader digitalization strategy, the alignment with other digital initiatives, and the potential impact on the digital ecosystem.

Expert	Need for National Digital Identity	Complexities involved	Current state of development	Potential Barriers	Role of E-Governance	Learning from early adopters	Digitalization strategy
Mogens Andersen	Potential Benefits of NDI.	Difficulties of catering to diverse user groups.	Implementation of MitID, replacement of NemID, planned integration of an EU wallet into the national infrastructure.	Low adoption rates, potential population barriers in larger countries	Free eID to citizens and incentivizing service providers.	De-centralization, self-sovereign identities.	Leverage private sector, use phased rollout approach.

Table 3 Interview Codes - Mogens Andersen

Expert	Need for National Digital Identity	Complexities involved	Current state of development	Potential Barriers	Role of E-Governance	Learning from early adopters	Digitalization strategy
Jen Schoedt	Reduces dark economy, simplifies the bureaucratic process,facilitates business continuity.	Data privacy and security concerns	Expanding through many more use cases of MitID	Coordination among organizations, legal and regulatory issue, lack of public awareness	Deployment and promotion through e-governance	Need for phased approach and interoperability with other systems.	Public-private partnership. Good marketing.

Table 4 Interview Codes - Jens Schoedt

Expert	Need for National Digital Identity	Complexities involved	Current state of development	Potential Barriers	Role of E-Governance	Learning from early adopters	Digitalization strategy
Srikanth Nadhamuni	Digital inclusion. Increased access to bank accounts in India.	Concerns about the centralization of data and security of user data	Aadhar has been integrated with a range of government services. 1.2+ billion registered users	Challenges related to diverse and large population in India. Illiteracy rate in rural part.	Digital Aadhar is being used to promote use of digital payments. Aadhar as an identification for financial transaction.	EU has a very high literacy rate as compared to other developing nations.	Implementing robust security measures. Complying with relevant privacy laws and regulations.

Table 5 Interview Codes - Srikanth Nadhamuni

Expert	Need for National Digital Identity	Complexities involved	Current state of development	Potential Barriers	Role of E-Governance	Learning from early adopters	Digitalization strategy
Siddhartha Arora	Improved accessibility for those who may have difficulty obtaining physical documents.	Importance of accuracy, reliability, and usability.	100% of adult population has Aadhaar. Biometric + fingerprint + Iris scans for authentication.	Lack of trust in public authorities. Financial burden on government.	Improving transparency, accountability, and communication to build trust between government and citizens.	Wide adoption. Interoperable solution. Decentralizing personal data through self-sovereign identity solutions.	Integrating Aadhar with systems such as tax filing. Setting up mobile enrollment centers to increase adoption.

Table 6 Interview Codes - Siddhartha Arora

6.3. Forming Sub-themes from coding

The codes were broadened into themes which increased the simplicity to analyze the data. The themes were divided into as - **Current state of development in National Digital Identity, Potential barriers that prevent diffusion, Lessons from early adopters, and Effective strategies to implement.**

The current state of development in National Digital Identity will summarize what are the latest solutions up to. What are countries looking for?

Potential barriers that prevent diffusion represent what are the obstacles/hurdles that prevent the diffusion of national digital identity.

Lessons from early adopters will summarize what learnings can developing countries take from the countries which are already pioneer in national digital identity solutions.

Effective strategy to implement summarizes what approach and digitalization strategy India can take to increase wide adoption of National digital Identity.

6.4. Finding based on comparative institutional analysis.

NDIDs	Country	Standards and Frameworks	Acceptance rate	Usage	Sources
eID	Switzerland	The ISO/IEC 29115:2013 framework	Low	Low	(Arora, 2008)
Aadhaar	India	e-Pramaan: Framework	High	Low	(S. Nadhamuni, personal communication, December 2022)
MitID	Denmark	NemID framework	High	High	(Mogensen, 2021), (A. Mogens, personal communication, November 2022)
BankID	Sweden	eIDAS, EU 910/2014	High	High	(Eaton et al., 2018)

Table 7 Comparative institutional study

Table 6 presents a comparative institutional analysis of different national digital identification systems. It includes information about the country, the standards and frameworks used, the acceptance rate, and the sources of information. Each system represents a specific country's approach to digital identity. In Switzerland the low acceptance rate suggests that the eID system was not widely adopted and integrated into various sectors and services within the country. While the acceptance rate of Aadhaar, India's national digital identification system, is indeed high, it is worth noting that the usage of Aadhaar vary and not up to the mark as compared to its acceptance. While Aadhaar has been widely accepted and integrated into various sectors and services in India, the level of individual usage is very low. This is certainly because of the factors and barriers discussed in literature part of this study. In pioneer countries like Denmark and Sweden the acceptance rate and use by its citizens has been very high. In Denmark transition from previous ID to new ID has been successful and the new system offers improved security and usability, meeting the needs of Danish citizens and businesses.

7. Analysis and Discussion

In the last chapter, findings of the qualitative expert interviews were presented, and following section will analyze this in relation to the literature and the theories used in this thesis along with the critical discussion. Throughout this chapter the answers to research question and sub-questions are provided.

The findings from chapter 6 will be used along with the literature in chapter 2 to answer the sub questions and main research question.

7.1. Sub RQ1: What is the current state of development in National digital identity in EU and India?

The adoption of national digital identity systems depends on various factors, including the specific goals and priorities of the country implementing the system, the level of technical infrastructure in place, and the level of support from the government and citizens. When discussing the current state of development in national digital identity in EU the experts had good knowledge about what's new and trending related to digital identities in the respective countries where they were from.

The use cases provided by MitID for citizens are – any tax system, any legal system, any financial system, any health care system, and any educational system whereas the use cases provided for businesses include - Public tax and VAT systems, Some financial systems, Public Mail system, Mail encryption, and Digital signing. Overall it support more than 500 systems as of now (Alling, 2022). In Demark currently, NemID is being replaced by MitID and the full migration is expected to be completed by 2024-25. In fact, you can no longer use the banking sector without migrating to MitID (A. Mogens, personal communication, November 2022). There have also been efforts to expand the use of digital identity in Denmark beyond just government services, with the goal of creating a more comprehensive and interoperable system that can be used across a wide range of sectors and as a result of this the new MitID is also an eIDAS compliant solution (J. Schoedt, personal communication, December 2022).

The Aadhaar program has seen around more than 1.3 billion enrollments i.e. almost 90% India's population already has an unique identity in the form of digital Aadhaar which has provided nearly around 300 use cases in last 10 years (S. Nadhamuni, personal communication, December 2022). The Aadhaar authentications have been growing steadily in fact in February 2018, 271 million individuals used their Aadhaar to authenticate themselves, representing nearly one in four people in possession of an Aadhaar (Abraham et al., 2018).

The research has found that the use cases for national digital identity solutions are increasing day by day and countries are making sure that their solution for digital identity lives up to the expectations and the need of the citizens. The national digital identity solution in some countries of EU specifically in Estonia, Denmark and Sweden are technically more advanced and serves far more use cases as compared to India's digital Aadhaar. Efforts have been made to build decentralized identity systems based on the self-sovereign identity principles which are interoperable among different countries.

7.2. Sub RQ2: What are the potential barriers that prevent the diffusion of the National digital identity?

The research has found that there are a lot more barriers to the diffusion of national digital identity solutions. There are several barriers that can prevent a national digital identity system from functioning effectively. Barriers to achieving functioning in e-governance refer to the various challenges or obstacles that prevent the effective implementation and use of electronic governance systems. These barriers can be grouped into several categories, including technological, organizational, social, and cultural barriers (Madon, 2004)

Lack of trust - It is found that the people in developing countries like India do not have trust in their governments and hence does not tend to provide their personal data to the government. Whereas in a developed country of EU, the citizens have big trust in their government. This becomes the biggest barrier for developing countries if they want to roll out any e-governance service for their citizens (S. Arora, personal communication, December 2022) .

Awareness and knowledge gap- Mainly in developing country like India citizens are not aware of the benefits that the national digital identity solutions provided neither they understand how to use this solutions (Tsap et al., 2019). There is a big knowledge gap among Indians about the national digital identity schemes and it is very difficult to convince poor and illiterate people to make use of digital identity(Arora, 2008). Majority of Indians still use hard copies of Identity card to confirm their identity and can only avail offline services which almost makes impossible for them to use online services due to lack of understanding of using such online services.

Privacy concerns - Privacy is a major concern when it comes to national digital identity systems, as they typically involve the collection, storage, and sharing of personal information. There is always a risk of data breach and misuse of personal data. According to (J. Schoedt, personal communication, December 2022) it is important that national digital identity systems are designed and implemented with privacy in mind, and that they include robust safeguards to protect personal data and ensure that it is used only for appropriate purposes. EU has a strong privacy law called GDPR and it contributes to compliance while building identity systems. Whereas in India the law is the "Personal data protection bill" and it is currently under the review of the parliamentary committee.

Population - From the research, it is found that all the pioneer and successful countries in national digital identity solutions are the ones that are smaller ones and have less population. It becomes difficult to scale a solution to a larger population and to maintain and update the record over time (S. Nadhamuni, personal communication, December 2022). More the population more it is difficult to scale the solution since the number of authentication transaction increases which indeed requires substantial infrastructure and resources. Ensuring the accessibility and inclusion of all segments of the population is crucial for the success of identity solutions. India has a diverse demographics, including rural areas, remote regions, and economically disadvantaged communities. Reaching and providing digital identity services to these diverse populations is more complex due to geographical, cultural, and socioeconomic factors.

The study has also found other barriers like technical challenges, cultural and historical factors, organizational issues, and financial constraints.

7.3. Sub RQ3: What learnings can India take from the early adopters in Europe?

Designing a legal framework and strategy **-** A legal framework for national digital identity would provide the legal basis and guidance for the creation, issuance, use, and management of digital identities at the national level. It should outline the objectives and principles of the digital identity system, as well as the rights and responsibilities of the various stakeholders involved, including individuals, government agencies, and private sector organizations (J. Schoedt, personal communication, December 2022). Many developing countries yet do not have a privacy law like a GDPR. It is important to pass such law/act in the country so that citizens can trust the system and agree on sharing their data. Define a governance structure that outlines the roles and responsibilities of relevant government agencies, oversight bodies, and stakeholders involved in the national digital identity system. The governance structure should ensure transparency, accountability, and effective coordination among different entities. Consider creating an independent oversight body to monitor the system's compliance, address concerns, and maintain public trust.

Cultural and Historical factors **–** From studying the successfully deployed national digital identity solutions in EU it is evident that such solutions are diffused easily when you have a less population. In addition, Denmark embraces information technology and has a forward-thinking e-government strategy (S. Nadhamuni, personal communication, December 2022). The literature also suggests that a small country with a homogenous population may not face the same political resistance when proposing new technology projects that would be found in a more politically divided nation (Castro, 2011).

Policy issues **–** From the study, it is found that rolling out a national digital identity for its citizen is only the first step but what countries in EU have done differently is they have adopted the demand-side policies to increase the wide adoption of national digital identity solution i.e.

they have done investments in the e-government schemes which lets enhanced interaction between citizens and helps them utilize different use cases (J. Schoedt, personal communication, December 2022).

Technology issues **–** The experience and learnings from the existing solutions in EU suggests that it is advisable to build an interoperable solution so that citizens can use their own national identity solution to authenticate themselves throughout the EU member states (A. Mogens, personal communication, November 2022). When discussing the technological issues of national digital identity with the experts all of them talked about the interoperability.

Privacy and Data Protection - As mentioned in the literature section privacy advocates raise objections for the use of national digital identity solutions mentioning the threats to the liberty of citizens and increased monitoring of user's private data. Hence it is important to have strict privacy laws in place so that citizens data is secure. EU has GDPR which has a penalty of 4% of annual revenue in case of theft or fraud which is highest among all other laws currently passed by any country.

7.4. Main RQ: Despite the growth of digitalization, India does not have one common/standard login for both public and private self-service solutions. What can be an effective strategy/framework to increase the adoption of national digital identity in India?

As seen from the literature the demographics, cultural and historical factors have an impact on the country's national digital identity strategy. Although India is late in building its national ID strategy, if it takes the learnings from early adopters and set up its own strategy then it can capitalize on an opportunity to create a system that can enhance the digital economy of the country and overcome many obstacles it would face otherwise.

Design a Framework **–** This study brings up a new framework with the use of comparative institutional analysis and Christopher Allen's principles of Self-Sovereign identity. This framework suggests to study and compare different institutional arrangements and systems to

identify best practices and lessons learned. This framework also enables developing countries to understand how to adapt existing models to suit their unique socio-economic, cultural, and technological landscapes. It helps identify contextual factors that may influence the design, implementation, and acceptance of national digital identity solutions. Christopher Allen's principles of Self-Sovereign Identity provide a set of guiding principles for creating decentralized and user-centric identity systems. The blend of comparative institutional analysis and Allen's principles form a holistic framework that can help developing countries in adoption of digital identity.

Create an implementation plan - Identify and engage all relevant stakeholders, including government agencies, private sector organizations, and civil society groups. It is important to understand the needs and concerns of each stakeholder group and to involve them in the planning process. As per the discussion with the interviewee, the pioneer countries like Denmark, Sweden & Estonia involved the private sector to implement their solutions as the government alone cannot build a successful system without support from the private sector. India is a huge country with a population of around 1.3 billion and if we look at the pioneer countries have a population of around 6 to 10 million. Most of the countries which are pioneer in building such solutions are the smaller countries. One of the interviewees recommended that India should use a phased approach while rolling out digital identity features maybe starting from villages to the cities and then to the different states step by step to effectively manage the successful implementation.

Build a system that supports new technologies – The national digital identity should support wide range of use cases for its citizens and should be built on the latest technology framework so that it is long lasting solution. In EU new a new way of thinking about digital identity has emerged i.e., self-sovereign identity. The new EU digital identity wallet is compliant with the Christopher Allen's principles of SSI. All the interviewees involved in this research frequently mentioned that the national digital identity solution should be interoperable. As interoperability can facilitate innovation and the development of new products and services by enabling the integration of different technologies and platforms. And hence the system should be designed in a such a way that it can be easily integrated with other cross border systems.

Design a solution for National identity that maximizes benefits for users and providers – The national digital identity solution should be easy to use and navigate that guides user through easy authentication and authorization process. One of the interviewees specifically mentioned that the service provider should see the benefits out of these solutions so that they are interested to invest in such a system. According to (A. Mogens, personal communication, November 2022) the reason behind the slow adoption in some countries is the service providers can verify users but users can not verify the service providers i.e. the benefits are one sided.

Aim for disruptive innovation and not just diffusion – The developing countries can take the learning from the countries who have successfully implemented national digital identities. They can avoid the issues and difficulties faced by developed countries which they faced while implementing this at an early stage. Literature talks about the e-KYC process which helped Indian citizens to get bank accounts using Aadhaar which had a disruptive increment from 17 % to 80% from 2008 to 2021.

Integrate national digital identity into key services and transactions **-** Another effective strategy is to integrate national digital identity into key services and transactions, such as banking, healthcare, and social welfare. This can create a strong incentive for users to adopt the national digital identity (N. Vasita, personal communication, April 2023).

Provide citizen education and support – It is important to educate users about the national digital identity system, including how to use it, the data it collects, and the safeguards in place to protect their privacy. Government should take efforts to ensure the e-readiness of the country's citizens. Launch public awareness campaigns and educational initiatives to inform citizens about the benefits, functionalities, and safeguards of the national digital identity solution. Educate individuals about their rights, responsibilities, and the measures taken to protect their privacy and data (N. Vasita, personal communication, April 2023).

Conduct Pilots and Iterative Implementation- Europe has often adopted a phased approach, conducting pilot projects and iterative implementations of digital identity systems. India can follow this approach to test and refine its digital identity initiatives on a smaller scale before

scaling them up nationally, allowing for adjustments based on user feedback and lessons learned (N. Vasita, personal communication, April 2023).

The Indian digital Aadhaar system is built for the common man. The people who are literate or computer literate enough to login into banking are fairly a small minority. There are not a large number of people who log in to banks over their phones and computers. Right now, it is more important for India to make sure that people who don't have bank accounts get access to banking. And India did that with the digital Aadhaar – before 2008 only 17% of citizens had bank accounts and as of today almost 80% of citizens have bank accounts (S. Nadhamuni, personal communication, December 2022). Considering the unawareness about the national digital identity and its use for authentication to the people of India is very difficult to make them use such solutions. Especially when the citizens do not have trust in the government for financial activities (Tsap et al., 2019). For now, India is not looking at the centralized or federated identity system since user's identity is in the hands of someone else in these cases. India is looking forward to building a national digital identity authentication service which is a decentralized identity so that the user itself is the sovereign of their own identity(S. Shetty, personal communication, April 2023). India's requirement as a country towards national digital identity is very different at this stage as compared to countries in EU where the literacy rate is very high and its citizen know how to do banking through phones and computers(S. Shetty, personal communication, April 2023). From the discussion with the Indian Interviewees, it was pretty evident that use of digital Aadhaar for authentication and single login solution is not a burning need as of now in the country and even if such a solution is rolled out people might not use it. But interviewees also mentioned that looking at the benefits and advantages the national identity solution as an authentication method provides are huge and India will definitely have such a solution in place in future.

8. Conclusion

The main objective of this research was to understand what can be an effective strategy/framework to increase the adoption of national digital identity in India? And to achieve this objective it was necessary to get answer to three sub questions. With the help of relevant theories and framework I was able to achieve the objectives of this research by getting answers to all research questions: (1) What is the current state of development in National digital identity in EU and India?; (2) What are the potential barriers that prevent the diffusion of the National digital identity?; (3) What learnings can India take from the early adopters in Europe?

The results of first research question helped to understand the current state of developments in digital identities in EU and in India which helped to compare both the regions based on the solutions and understand where these countries are at present with respect to their national digital identity solutions. The results of second research question helped to understand the barriers that prevent the adoption of national digital identity in a country. Many different obstacles that hinder the adoption of national digital identity came to limelight from the literature as well as from the interviews. The third research question addresses the learnings that a developing country should take from the early adopters so that they can effectively implement such solutions in their own countries. The results of this research question are helpful for the developing countries so that they do not face the same issues which early adopter came across. The results of the main research question helped to build an effective strategy for developing countries to increase adoption of national digital identity solution. This can help the developing countries to set up its own strategy and capitalize on an opportunity to create a system that can enhance the digital economy of the country.

9. Reference List

Abraham, R., Bennett, E. S., Bhusal, R., & Dubey, R. (2018). *STATE OF AADHAAR REPORT* (p. 54). IDinsight. https://stateofaadhaar.in/assets/download/State_of_Aadhaar_Report_2017-18.pdf

Allen, C. (2016). *Self-sovereign-identity*. Web of Trust Info. https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/11305e490f8a502024f7478e502540bd1d4cc931/self-sovereign-identity-principles.md

Alling, B. (2022, May 11). *Denmark's 2022 brand new eID solution*. European identity and cloud conference. https://www.kuppingercole.com/sessions/5016/1

Andermatt, K. C., & Göldi, R. A. (2018). Introducing an Electronic Identity: The Co-design Approach in the Canton of Schaffhausen. *Yearbook of Swiss Administrative Sciences*, *9*(1), 41. https://doi.org/10.5334/ssas.122

Arora, S. (2008). National e-ID card schemes: A European overview. *Information Security Technical Report*, *13*(2), 46–53. https://doi.org/10.1016/j.istr.2008.08.002

Arora, S. (2022, December). *Principal Customer Success Manager at IBM* [Personal communication].

Banerjee, S. (2016). *Aadhaar: Digital Inclusion and Public Services in India* (p. 16). World Development Report. https://thedocs.worldbank.org/en/doc/655801461250682317-0050022016/original/WDR16BPAadhaarPaperBanerjee.pdf

Bell, E., Bryman, A., & Harley, B. (2022). *Business Research Methods*. Oxford University Press.

boyd, danah. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Brunel University, & McGrath, K. (2016). Identity Verification and Societal Challenges: Explaining the Gap Between Service Provision and Development Outcomes. *MIS Quarterly*, *40*(2), 485–500. https://doi.org/10.25300/MISQ/2016/40.2.12

Casper, S., & Whitley, R. (2004). Managing competences in entrepreneurial technology firms: A comparative institutional analysis of Germany, Sweden and the UK. *Research Policy*, *33*(1), 89–106. https://doi.org/10.1016/S0048-7333(03)00100-8

Castro, D. (2011). *Explaining International Leadership: Electronic Identification Systems* (p. 70). THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION. https://www2.itif.org/2011-e-id-report.pdf

DIGST.dk. (2021). *The key to Denmark's digital success*. Denmark.Dk. https://denmark.dk/innovation-and-design/denmarks-digital-success

Eaton, B., Hedman, J., & Medaglia, R. (2018). Three Different Ways to Skin a Cat: Financialization in the Emergence of National e-ID Solutions. *Journal of Information Technology*, *33*(1), 70–83. https://doi.org/10.1057/s41265-017-0036-8

European Commision. (2020). *European Digital Identity*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

European Commission. (2019). *Shaping Europe's digital future | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en

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

European Union, 119 OJ L (2016). http://data.europa.eu/eli/reg/2016/679/oj/eng

Ezawa, Y., Kakei, S., Shiraishi, Y., Mohri, M., & Morii, M. (2023). Blockchain-based cross-domain authorization system for user-centric resource sharing. *Blockchain: Research and Applications*, 100126. https://doi.org/10.1016/j.bcra.2023.100126

Felcourt, G. (2022). *On the road to User-Centricity: Digital Identity in the Electronic Wallet era* (p. 86). Security Identity Alliance. https://secureidentityalliance.org/utilities/news-en/on-the-road-to-user-centricity-digital-identity-in-the-electronic-wallet-era-1

Freeman, R. E., Harrison, J. S., Wicks, A. C., Parmar, B. L., & Colle, S. de. (2010). *Stakeholder Theory: The State of the Art*. Cambridge University Press.

Gable, G. G. (1994). Integrating case study and survey research methods: An example in information systems. *European Journal of Information Systems*, *3*(2), 112–126. https://doi.org/10.1057/ejis.1994.12

Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. *Frontiers in Blockchain*, *2*. https://www.frontiersin.org/articles/10.3389/fbloc.2019.00017

Göransson, A. (2018). *Electronic Identification as an Enabling or Obstructive force: The general public's use and reflections on the Swedish e-ID*. http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-77052

Hayes, A., Mann, S., Aryani, A., Sabine, S., Blackall, L., Waugh, P., & Ridgway, S. (2013). Identity awareness and re-use of research data in veillance and social computing. *2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmediated Reality in Everyday Life*, 51–58. https://doi.org/10.1109/ISTAS.2013.6613101

Kaneriya, J., & Patel, H. (2020). A Comparative Survey on Blockchain Based Self Sovereign Identity System. *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 1150–1155. https://doi.org/10.1109/ICISS49785.2020.9315899

Kő, A., Francesconi, E., Anderst-Kotsis, G., Tjoa, A. M., & Khalil, I. (Eds.). (2019). *Electronic Government and the Information Systems Perspective: 8th International Conference, EGOVIS 2019, Linz, Austria, August 26–29, 2019, Proceedings* (Vol. 11709). Springer International Publishing. https://doi.org/10.1007/978-3-030-27523-5

Kornelakis, A., & Hublart, P. (2022). Digital markets, competition regimes and models of capitalism: A comparative institutional analysis of European and US responses to Google. *Competition & Change*, *26*(3–4), 334–356. https://doi.org/10.1177/10245294211011295

Madon, S. (2004). Evaluating the Developmental Impact of E-governance Initiatives: An Exploratory Framework. *The Electronic Journal of Information Systems in Developing Countries*, *20*(1), 1–13. https://doi.org/10.1002/j.1681-4835.2004.tb00132.x

Madon, S., & Schoemaker, E. (2021). Digital identity as a platform for improving refugee management. *Information Systems Journal*, *31*(6), 929–953. https://doi.org/10.1111/isj.12353

Marangunić, N., & Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. *Universal Access in the Information Society*, *14*(1), 81–95. https://doi.org/10.1007/s10209-014-0348-1

Masiero, S., & Bailur, S. (2021). Digital identity for development: The quest for justice and a research agenda. *Information Technology for Development*, *27*(1), 1–12. https://doi.org/10.1080/02681102.2021.1859669

Miguel, G. (2019). E-Estonia: The e-government cases of Estonia, Singapore, and Curaçao. *Archives of Business Research*, *7*(2). https://doi.org/10.14738/abr.72.6174

Mogens, A. (2022, November). *Chief technical architect for MitID at the agency for digitization* [Personal communication].

Mogensen, T. K. T. (2021). *A security analysis of MitID*. 19.

Mooij, A. M. (2023). Reconciling transparency and privacy through the European Digital Identity. *Computer Law & Security Review*, *48*, 105796. https://doi.org/10.1016/j.clsr.2023.105796

Nadhamuni, S. (2022, December). *Founder and CTO of Aadhaar* [Personal communication].

NIST. (2017). *NIST* (NIST SP 800-63-3; p. NIST SP 800-63-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

Ochieng, P. A. (2009). AN ANALYSIS OF THE STRENGTHS AND LIMITATION OF QUALITATIVE AND QUANTITATIVE RESEARCH PARADIGMS. *Problems of Education in the 21st Century*, *13*.

Podgorelec, B., Alber, L., & Zefferer, T. (2022). What is a (Digital) Identity Wallet? A Systematic Literature Review. *2022 IEEE 46th Annual Computers, Software, and*

Applications Conference (COMPSAC), 809–818. https://doi.org/10.1109/COMPSAC54236.2022.00131

Pranav, M. (2018, September 27). Explained: You and your Aadhaar. *The Indian Express*. https://indianexpress.com/article/explained/aadhaar-validity-supreme-court-verdict-mobile-bank-number-linking-5376171/

Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity*. Manning Publications.

Puthal, D., Ranjan, R., Nanda, A., Nanda, P., Jayaraman, P. P., & Zomaya, A. Y. (2019). Secure authentication and load balancing of distributed edge datacenters. *Journal of Parallel and Distributed Computing*, *124*, 60–69. https://doi.org/10.1016/j.jpdc.2018.10.007

Rogers, E. M. (1983). *Diffusion of innovations* (3rd ed). Free Press ; Collier Macmillan.

Sao, P. C. (2013). *The Unique ID Project in India: An Exploratory Study*.

Schoedt, J. (2022, December). *Director of Business Development, eSecurity Services & Digitisation at Nets Group.* [Personal communication].

Shetty, S. (2023, April). *Architect at India Stack, Advisor – Ministry of Finance, India.* [Personal communication].

Stefan, B. (2020). *The European Digital Identity Framework*. https://www.worldbank.org/content/dam/photos/1440x300/2022/feb/eID_WB_presentation_BS.pdf

Sullivan, C. (2018). Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review*, *34*(4), 723–731. https://doi.org/10.1016/j.clsr.2018.05.015

The Aadhaar Act, 36 (2016). https://prsindia.org/files/bills_acts/bills_parliament/2016/Aadhaar_Bill,_2016.pdf

Tsakalakis, N., Stalla-Bourdillon, S., & O'Hara, K. (2019). Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised? In E. Kosta, J. Pierson, D. Slamanig, S. Fischer-Hübner, & S. Krenn (Eds.), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers* (pp. 255–274). Springer International Publishing. https://doi.org/10.1007/978-3-030-16744-8_17

Tsap, V., Pappel, I., & Draheim, D. (2019). Factors Affecting e-ID Public Acceptance: A Literature Review. In A. Kő, E. Francesconi, G. Anderst-Kotsis, A. M. Tjoa, & I. Khalil (Eds.), *Electronic Government and the Information Systems Perspective* (Vol. 11709, pp. 176–188). Springer International Publishing. https://doi.org/10.1007/978-3-030-27523-5_13

UIDAI. (2022). *A UNIQUE IDENTITY FOR THE PEOPLE* (p. 18). Unique Identification Authority of India. https://uidai.gov.in/images/Aadhaar_Brochure_July_22.pdf

Vasita, N. (2023, April). *Co-Founder & CEO at Trential* [Personal communication].

White, O., & Madgavkar, A. (2019). *DIGITAL IDENTIFICATION: A KEY TO INCLUSIVE GROWTH* (p. 32). McKinsey & Company. https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.ashx

World bank. (2019). *Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable*. World Bank.

https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

Wunderlich, F., Vries, J., & Kirilof, N. (2022). *DIGITAL IDENTITIES IN EUROPE ANALYSIS, IMPLICATIONS AND OUTLOOK OF THE DEVELOPMENT OF NATIONAL OBSTACLES TO INTERPRETATION AND IMPLEMENTATION* (p. 48). Arkwright Consulting AG. https://uploads-ssl.webflow.com/61509dd26eb1ae688f25b0d8/62b59f24387174848f6657ec_ARKWRIGHT-REPORT-EIDs-IN-EUROPE-062022.pdf

10. Appendix

10.1. Interview Summaries

Nilesh Vasita Interview summary

1. **How do institutional frameworks and governance structures impact the development and adoption of digital identity solutions in different countries?**

   Institutional frameworks and governance structures play a crucial role in shaping the development and adoption of digital identity solutions in different countries. In countries with strong legal and regulatory frameworks, digital identity solutions are more likely to be widely adopted and trusted by citizens and businesses.

2. **What are the key differences in governance structures between the EU and India when it comes to digital identity, and how do these differences affect the design and implementation of national eID solutions?**

   The governance structures for digital identity in the EU and India differ in several ways. While the EU has established a common legal framework for eIDs, India has adopted a federated approach with a centralized registry of citizens' identity data. These differences have implications for the design and implementation of national eID solutions, such as the level of interoperability and the extent of data sharing.

3. **To what extent are users involved in the design and development of digital identity systems, and how does this impact trust and adoption?**

   Users play a crucial role in the design and development of digital identity systems. Involving users in the process helps to ensure that the systems are user-friendly, secure, and meet their needs. When users have a say in how their identity is managed, they are more likely to trust and adopt these solutions.

4. **How can developing countries like India adapt existing digital identity frameworks to meet their specific needs and challenges?**

   Developing countries like India can adapt existing digital identity frameworks to meet their specific needs and challenges by focusing on interoperability and scalability. This can be achieved by adopting open standards and leveraging existing technologies to build a secure and interoperable digital identity infrastructure that can be easily scaled to meet the needs of millions of users.

5. **What are the key security and privacy concerns associated with digital identity systems, and how do different countries address these concerns?**

   Key security and privacy concerns associated with digital identity systems include the risk of identity theft, unauthorized access, and data breaches. These concerns are addressed by implementing strong authentication mechanisms, encryption, and access controls. EU has established legal frameworks that regulate the collection, use, and storage of personal data to protect individuals' privacy rights.

6. **How do national eID solutions in the EU and India incorporate the principles of security and privacy by design?**

   These solutions are designed with security and privacy in mind from the outset, incorporating features such as strong authentication mechanisms, encryption, and access controls. User consent and control over personal data are key principles in any eID solutions.

7. **To what extent are digital identity solutions interoperable and standardized across different countries and regions, and what impact does this have on cross-border e-governance and public service delivery?**

   Digital identity solutions are not yet fully interoperable and standardized across different countries and regions in EU. Lack of standardization and interoperability can hinder cross-border e-governance and public service delivery, as it can lead to duplication of efforts and increase the cost of implementing digital identity solutions. Efforts are underway to establish global

standards for digital identity, which would help to ensure interoperability and facilitate cross-border service delivery.

8. **How can standardization efforts be coordinated across different countries and regions, and what challenges arise in these efforts?**

   Standardization efforts can be coordinated across different countries and regions through collaboration and partnerships among stakeholders, including government agencies, industry associations, and international organizations. However, challenges arise in these efforts, such as differences in legal frameworks, cultural norms, and technical infrastructure. To overcome these challenges, stakeholders must work together to establish common principles and standards for digital identity, while also accounting for local context and needs.

9. **What are the benefits and drawbacks of using common login solutions for public and private self-service solutions, and how do different countries approach this issue?**

   Using common login solutions for public and private self-service solutions can enhance user convenience and improve access to services. However, it also raises concerns around privacy, security, and data protection.

10. **How can digital identity solutions be designed to maximize user adoption and trust, and what are some of the key best practices in this area?**

    Digital identity solutions can be designed to maximize user adoption and trust by prioritizing user experience, privacy, and security. Best practices in this area include involving users in the design and development process, providing clear and transparent information about how user data will be used and protected, and implementing strong security measures such as two-factor authentication and encryption.

11. **To what extent do cultural factors impact user adoption of digital identity solutions, and how can these factors be taken into account in the design and implementation of national eID solutions?**

Cultural factors can have a significant impact on user adoption of digital identity solutions, including factors such as attitudes towards technology, trust in government and other institutions, and preferences for certain types of user experiences. These factors must be considered in the design and implementation of national eID solutions by conducting user research and engaging with diverse stakeholder groups to better understand their needs and preferences.

Siddhartha Shetty Interview summary

1. **How do institutional frameworks and governance structures impact the development and adoption of digital identity solutions in different countries?**

   Institutional frameworks and governance structures are critical to the success of national digital identity solutions. Clear legal and regulatory frameworks help to establish trust and confidence in these solutions, which is essential for widespread adoption. Effective governance structures ensure that these solutions are developed and implemented in a secure, transparent, and user-centric manner.

2. **What are the key differences in governance structures between the EU and India when it comes to digital identity, and how do these differences affect the design and implementation of national eID solutions?**

   EU has developed a common legal framework like GDPR for data privacy and moving towards Digital identity wallets which is a decentralized approach using self-sovereign identity principles. Whereas India has a centralized registry of identity system.

3. **To what extent are users involved in the design and development of digital identity systems, and how does this impact trust and adoption?**

   The involvement of users in the design and development of digital identity systems is critical to building trust and driving adoption. When users have a

voice in the process, it helps to ensure that the systems are user-centric, secure, and meet their needs.

4. **How can developing countries like India adapt existing digital identity frameworks to meet their specific needs and challenges?**
   By tailoring them to their specific needs and challenges. This can be achieved by the experiences and lessons learned from the other countries. Collaboration between governments, private sector and civil society can help to identify and address unique challenges.

5. **What are the key security and privacy concerns associated with digital identity systems, and how do different countries address these concerns?**
   Risk of data breaches, identity theft and unauthorized access are the key issues. EU is moving towards decentralization of identity to tackle this key issues. And every country must do that.

6. **What are the potential barriers that prevent the diffusion of such a technology?**
   Population of a country is one of the barriers. Country population in EU is in few millions whereas in India alone the population is over one billion. Literacy rate is another barrier. Digital technology awareness is far less in developing countries and hence citizens have no knowledge to use such a technology.

7. **How can developing countries adjust their digitalization strategy to increase adoption of national digital identity?**
   Many countries in EU provided eID free of cost to its citizens. Establishment of legal frameworks is the base for successful implementation of eID system. Setup large number of use cases that eID can support. You must create mass distribution of services using the private sector, because this is where people actually use it. Asking people what obstacle they face and then providing them a good use case for it. Roll out the service first in cities and then go on launching

them in other cities in batches to better understand the solution and its complexities.

8. **What is the role of e-governance in diffusion of national digital identity solution?**

   Government should try to make service providers interested so that they find some financial interest in making such service available to users. E-governance infrastructure can provide a platform for the deployment of a national digital identity system, enabling it to be accessed by citizens and businesses from any location.

9. **Why cross border identity solutions matter?**

   It lets people to authenticate and access services regardless of their geographical location. Mainly for international remote workers, travelers and global businesses who uses resources and services from other parts of world.

10. **To what extent do cultural factors impact user adoption of digital identity solutions, and how can these factors be considered in the design and implementation of national eID solutions?**

    There are factors like attitude towards technology, trust in government and institutions and it can be taken into account by conducting user research. Linguistic diversity should also be considered so that every citizen understands and can use the system. Investment in campaigns and education initiatives must be done which should be tailored as per the cultural contexts.