14th of May 2018

INTEROPERABILITY FOSTERING INNOVATION

An Electronic Identification Initiative

Students

Alma Gudny Arnadottir

Erika Michelle Pinto

Master Thesis

MSc Business Administration & Information Systems (e-Business)

Supervisor

Jonas Hedman

No. of Pages: 80

No. of characters:170.096

“

“Information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without the talking about the other”

- Bill Gates

ABSTRACT

This paper sought to make a contribution to understand how interoperability can foster innovation when tailored to the field of electronic identification. The research included actors from four start-ups in Denmark. The concept of interoperability (Gasser & Palfrey, 2012) was the theoretical base on which research was conducted. It is a holistic approach that includes layers such as data, technology, human and institution. Additionally, this paper developed a conceptual framework from which to investigate interoperability and innovation and aimed to answer the question of '*How does interoperability foster innovation through electronic identification (e-ID) systems?'* The research method used was semi-structured interviews. The findings state that interoperability led to innovation in the context of e-ID. On further investigation it became evident that there were factors that foster innovation in e-ID. The factors found were increased efficiency, increased trust and security, less resources spent and increased collaboration. Collectively, these factors led to improved validation. Based on the identified factors a solution was built. The resulting solution was an interoperable innovative e-ID solution. The solution included multiple attributes or verification points that businesses can use to create a safe and efficient digital ecosystem for their users. It was created based on the interoperability layers and therefore resulted in the solution being a cloud based Blockchain that can be accessed via an API. In the discussion, recommendations are provided for a potential solution by presenting a prototype of an e-ID system and implications of the research discussed.

Keywords - Electronic Identification, interoperability, digital innovation, digital technologies, start-ups.

ACKNOWLEDGEMENTS

We wish to thank the five actors interviewed for their cooperation, collaboration and for providing us with insightful information on the topic. Their ideas were valuable which made this whole process a dialogue. Their help and effort, made the thesis what it is today. We also want to thank those who proofread the thesis and helped us with their valuable suggestions. Furthermore, we want to thank our supervisor Jonas Hedman. Without his guidance and supervision, the process would have been difficult. We appreciate his help and encouragement. We want to thank our family and friends for motivational encouragement throughout the process. Lastly, we want to thank Copenhagen Business School for the caffeine that made this process delicious.

Copenhagen, May 14th 2018,

Alma Gudny Arnadottir
Erika Michelle Pinto

1. INTRODUCTION

The global report on cybercrime and its economic impact by McAfee and CSIS (Centre for Strategic and International Studies) states that "...cybercrime costs businesses close to $600 billion, or 0.8 percent of global GDP, which is up from a 2014 study that put global losses at about $445 billion" (McAfee, 2018). Digital technologies have been transforming the way organizations conduct business online. With this transformation users and customers have altered the way they interact with businesses and other users. Although these technologies improve our lives, we as stakeholders are vulnerable due to the actions of individuals who maliciously use technology. As stated by Davis "in simpler times, passwords broke down physical barriers they allowed people into secret gatherings, opened safes, the list goes on. Enter the digital era, and passwords now act as the gatekeepers to our personal data, as they lock down everything from our social media accounts to our email inboxes" (Davis, 2018).

Moving toward a future where we will be more dependent on technology than ever before is thought-provoking. According to Gasser & Palfrey (2012), the habituation of technology in our daily lives calls for even more digital interconnectedness. When a device does not work the way we want it to, we are paralyzed or displeased. Linking these diverse ideas, the underlying need is to support the creation of a digital ecosystem that is safe, secure and efficient. By doing so, the focus can move toward innovation. Based on the aforementioned idea, we look into the interconnectedness we permit from technology through the perspective of the user and a business. Focusing on electronic identification (e-ID) as a driver for digital safety, security and efficiency.

E-ID is a topic in early development but gaining increased awareness, world over. E-ID influences different stakeholders, such as governments, businesses and individuals. Thus, it is relevant, to develop an identification system wherein, all stakeholders involved in the process can contribute to optimize the beneficial usage of the system (Palfrey & Gasser, 2007b). Electronic identity can be classified as a solution to the problem of identification, giving access to various services, public and private, in an increasingly digitized world. According to the Universal Declaration on Human Rights "everyone has the right to recognition everywhere as a person before the law". However, it is estimated that 1.1 billion people all over the world are unable to prove who they are (ID2020, 2018; World Bank, 2018).

The western world has the potential to capture on current advancements in technology to develop an e-ID system. One that can provide and maintain electronic identities so that all individuals can be part of the digital economy. Such as "a trusted, secure and universally accepted digital identity fosters economic growth, productivity and financial inclusion" (Macknight, 2018). Furthermore, as e-ID is gaining momentum, one of the sustainable development goals (2015-2030) of the United Nations (UN) is to "provide legal identity to all, including birth registration, by 2030". This includes over 20 million refugees worldwide. An e-ID bringing the individual at the centre might lead to many opportunities such as political, economic and social benefits (ID2020, 2018). In a world where identification electronically becomes a part of our daily lives there is a need to leverage the full potential of this identity. E-ID can be considered as a "service of all services", where it provides a service that kick-starts all other digital services, in the interest of all stakeholders involved (Medaglia et al., 2017). However, there are certain forces that come into play when addressing e-ID. The forces can enable and/or hinder the development process and, therefore, essential to mention.

1.1. FORCES AT PLAY

Concerns about data security, privacy and trust coupled with the need for individuals to identify themselves, permits e-ID to lead the way. However, developing an identity solution that allows for harmonization can prove complex. Therefore, the forces need to be taken into consideration for mitigation of risk and managing expectations. The forces that affect positively or negatively the development process are (1) Regulations and legal diversity (2) Technology and (3) Social factors. These forces are prominent when developing an e-ID system that accounts for the global user.

Legal diversity is a force in developing an e-ID system as there are different legal requirements depending on countries. On a government level there have to be incentives to create interoperability between countries (Palfrey & Gasser, 2007b). In Europe, the 'electronic identification of trust and service for electronic transactions in the internal market' (eIDAS) marks a milestone in creating a framework for member states to build an interoperable e-ID system for the public and private sector (European Commission, 2017). However, e-ID contains sensitive personal data and has to follow regulations such as the 'general data protection regulation' (GDPR) (European Commission, 2018a). These regulations collectively indicate an initiative that is indicative of trust for citizens and puts the user in control of his or her identity.

Following legal diversity is technology, a force impacting the development of an e-ID. New technology is constantly being developed such as the distributed ledger technology (e.g. Blockchain), cloud computing, biometrics and artificial intelligence (AI). However, the adoption of such technology differs depending on the country and their culture. An e-ID system built on the right technology increases efficiency and enables innovation within both the public and the private sector. Furthermore, an effective e-ID infrastructure might ease the development of a digital economy (World Bank, 2018). Yet, there is a gap between the public and private sector. Government involvement in developing an interoperable ID system might take a long time and hinder technological development (Palfrey & Gasser, 2007b).

Conclusively, adhering to regulations is important because an e-ID system includes sensitive data about citizens and businesses. The issue of liability is important in an age where data breaches are frequently increasing. There are inherent differences in national and international legislation that need to be fulfilled. Technology differs regarding cost, complexity and security which affects its adoption. Furthermore, it is essential to take other forces into consideration, such as social factors, including culture and market maturity (World Bank, 2018; Palfrey & Gasser, 2007b). These forces raise awareness and concerns. Based on which, the next section will illustrate the research problem and how that led to the development of the research question.

1.2. RESEARCH PROBLEM

The problem in the field of e-ID is the issue of multiple schemes for identification and the lack of harmonization between them. Each of the schemes developed until now have different capabilities and fulfil different requirements. The problem that these e-ID schemes have in common is the lack of interoperability between them. In the context of e-ID, there has been no coordination among countries in developing systems together (Arora, 2008). Therefore, e-ID differs from country to country because of diverse regulations, technology and culture. However, the European Union is taking the step in the right direction with the eIDAS regulation (European Commission, 2017). The issue here is that the framework is generic in nature and does not allow to leverage the full potential that interoperability can bring with it. Additionally, with businesses operating in international markets these national identity schemes do not fulfil the business needs. Because of lack of alignment of systematic process of implementing a standardized e-ID across the world, it has led to different types of national e-ID systems (Arora, 2008).

To develop a coherent e-ID various actor have to work together, such as the private sector, regulators, and society. Increased interoperability between these actors can potentially lead to opportunities and enable a beneficial system for individuals, devices and private firms (Palfrey & Gasser, 2007a). Furthermore, the question of who should take the initiative in developing such a system is still to be determined. Both private and public actors have the potential to develop a system or scheme that can resolve the lack of interoperability issue. Even though companies can achieve goals by working together this is not always the case. To work together, there needs to be an alignment of work processes and information systems. Additionally, the individuals that control these systems and conduct these processes need to work together despite cultural and personal differences (Palfrey & Gasser, 2012). Previous research on e-ID development has shown that there are problems in implementing such system because of lack of interoperability in relation to private-public coordination. Another example has shown lack of uptake of an e-ID system issued by the government because of existing commercial e-IDs initiated by the private sector (Hoff & Hoff, 2010; Rissanen, 2010). In both cases, the problems can be tracked to lack of interoperability within the human and institution layers. Additionally, this demonstrates two worlds clashing in e-ID development. This further illustrates the development of an e-ID as a collaboration of individuals and technology.

Launching e-IDs for citizens and businesses is very important for the governments to realize e-government policies and to provide better services to citizens in an efficient, secure and trusted way on national as well as imminent transnational levels. Kubicek and Noack (2010a, p. 237) describe the rollout phases of e-ID projects and reflect upon the choices of different solutions for e-IDs and digital signatures. According to the ID4D (World Bank Group, 2016), there needs to be a public-private partnership. However, while acknowledging that the government is extremely vital in the development and roll out of an e-ID scheme, here the focus is on the contribution that the private sector can provide. Based on the lack of harmonization between schemes and the need for a public-private partnership, the next section will introduce the research question.

1.3. RESEARCH QUESTION

Due to the lack of harmonization between e-ID schemes due to diverse regulations and technology the problem of interoperability arises. By identifying the problem area, a certain gap has been pinpointed. This has been classified as the lack of interoperability across e-ID schemes and the lack of research through the perspective of private businesses (Arora, 2008). On the basis of this the following research question is developed:

How does interoperability foster innovation through electronic identification (e-ID) systems?

There exists plenty of research on the topic surrounding public-private partnerships (Medaglia et al., 2017), here the focus is on the private sector. In this study actors within the private sector more specifically start-ups were interviewed on their view on the topic of interoperability across electronic identification. The actors interviewed are involved in private companies based in Denmark and operate in the international market. However, the aim of the research is to discover how interoperability can encourage or foster innovation when applied to the field of e-ID. To answer the research question, the concepts of interoperability, electronic identification and innovation will be addressed.

The research addresses the concept of e-ID through the theory of interoperability by Palfrey and Gasser (2012). The assumption throughout the paper is that interoperability leads to innovation. Nonetheless, the aim is to find which components foster innovation specific to e-ID. Furthermore, underlying factors such as technology, regulations and culture are taken into consideration. It is important to have in mind that the concept of e-ID, is new and still in early development. Therefore, the readers of this paper should bear in mind that the research is a snapshot in time. As such, highlighted challenges and limitations for businesses in the private sector in the report might not be the same as today and the years to come. The novelty of the research from the perspective of the private sector coupled with the fact that it is a global issue fuelled our motivation to investigate.

The paper will be structured as follows. In the next section previous literature related to the research question is reviewed. Then the main theory of the paper is addressed. Thereafter the research method is introduced followed by the analysis of the results. Next, the results are discussed through reflection based upon previously reviewed literature. The theoretical and practical contributions are stated and implications for future research are introduced. Finally, the conclusions of the research where main findings are highlighted and the research question is answered.

2. LITERATURE REVIEW

The aim of this section is to review existing literature applied to the topic to further support the claims espoused in our discussion. The section begins with the history of identification as it shows the evolution in technology and how that has shaped the field of e-ID. Following which the definitions are stated and various use cases introduced. Subsequently, literature on the concept of interoperability and innovation is presented which highlights its need in the field of e-ID. Lastly, the different e-ID schemes are reviewed.

2.1. HISTORY OF IDENTIFICATION

The documentation of individuals through various identification schemes dates back to ancient times. Prior to the introduction of a passport, individuals were documented after birth by the church. Following written documentation as records kept by the church came the birth certificates "as for passports, the credit for their invention can go to King Henry V of England in 1414 where he created the documents for English citizens who needed to prove their identity while in foreign countries. These papers were then referred to as "safe conduct" documents and ensured a citizen's safety in a neighbouring country when gifted by the monarch" (Trulioo, 2014). As populations increased and the demand for immigration grew the idea of the passport became more viable "this all changed in 1920, when the idea of a worldwide passport standard emerged in the aftermath of the First World War, championed by the League of Nations, a body tasked with the heavy burden of maintaining peace" (National Geographic, 2018).

The first record of social security number cards was in the United States in 1936. Over the next years other countries followed and later, in 1977, an electronic data processing system was developed. The purpose of the system was to monitor taxation and welfare of its citizens. This lead to the development of "smart cards" as an identity card. The purpose of the card was to incorporate some of the necessary public services into one card such as citizenship, finance and health care. Later on, with the increased usage of the Internet, multi-factor verification was introduced. The verification was first introduced by Google in 2011, where the user had to enter his or her username and password, followed by a unique code sent to the user's phone via text message. Identity verification has become crucial in many industries today, such as finance, with applicability for detecting online fraud and money laundering. The following table summarizes the evolution of identification schemes. It is important to state as the table suggests that identification of individuals or businesses for that matter is not a new concept and has been around since ancient times. However, the schemes of identifying have changed due to the change in requirements (Trulioo, 2014).

Table I: The history of Identity

Type of Identifier	Timeframe	Location
Jewellery or other decorative goods	100,000 years ago	South Africa, Israel & Algeria
Tattoos and Skin markings	2000 BC	Ancient Egypt
Written Census	209 BC	Rome
King Henry V invented true passport	1414	United Kingdom
Passport link to unique identifying number	1829	United Kingdom
The negative positive photographic system	1840	United Kingdom
Decentralized personal number system (PN)	1849	Netherlands
Use of Fingerprints as precise identification	1870	United Kingdom
Social Security Number card (physical)	1936	United States of America
Two Factor Verification for ATM	1960's	United States of America
Government issues Smart Cards	1980's	Germany, Singapore, Czech Republic and Spain

Know Your Customer (KYC) for financial institutions for AML programs	2001	United States of America
Automated Palm Print Database	2004	United States of America
Cyber Identity Verification	2009	Canada

The concept of e-ID has been in discussion since the Internet and email were adopted as communication in business, government and in leisure time (Kubicek, 2010). In the 1990s, Microsoft was the first actor to introduce a unified e-ID online with a passport product. It allowed users to login into different sites with one username and password. However, the endeavour was unsuccessful, as the company changed the name of the product multiple times and failed in certain tasks. This marked the first generation of online identity, namely "Identity 1.0". About ten years later, in 2010, the social media giant Facebook created a second generation of identity, "Identity 2.0", when allowing users to login to other websites by using their Facebook account. The login feature was a success, as businesses began to allow their customers to login through their social media account. Businesses today continue to develop identification features such as Apple's touch ID. Simultaneously, technological advancement allows different actors to work together by combining different components and devices. The private and public sector have tried to capitalize on technology and aim to create the third generation of identity, "Identity 3.0" (Salyer, 2015). Over the last two decades e-ID schemes have been in development across several countries. Today, over 60 countries have a national ID scheme, where most of them issue national e-ID cards. Such e-ID systems typically incorporate social security cards and in some cases driver's licenses or healthcare cards. It is expected that the number of national e-ID cards will be 3.6 billion in 2021 (Gemalto, 2018a; Gemalto, 2018b). Based on these initiatives, the underlying force that drives the development of identities is technology.

2.2. DEFINING E-ID

The concept of e-ID has been used in various contexts with different meanings. The term is often used in context with security and privacy, however, the significance varies depending on industry such as government, banking and commercial firms. Additionally, there is a difference between personal, organizational and national identification (Kubicek, 2010). Because of the different meanings of the concept of e-ID, the term will be defined and used accordingly in this study. The European Commission (EC) has adopted the following definition of electronic identification, e-ID is "*one of the tools to ensure secure access to online services and carry out* *electronic transactions in a safer way*" (European Commission, 2017). Kubicek (2010) identifies electronic identity as "*identity, which is represented by electronic means and/or readable by electronic devices*". Another definition of e-ID is a digital identity, where identity is explained as "*the dynamic collection of all of the entities attributes*" and a digital identity is defined as "*a partial identity in an electronic form*". Furthermore, a digital identity is made by subset of attributes where "*an attribute is a distinct, measurable, physical or abstract named property belonging to an entity*" (Modinis Study, 2005). The World Bank Group also refers to digital identity. They define the term as "*a set of electronically captured and stored attributes and credentials that can uniquely identify a person*" (World Bank Group, 2018). Another way to view identity is to break down the components it is built upon. In that sense, it can be divided into four categories: physical attributes (e.g. biometrics), legal representation (e.g. passport), electronic presence (e.g. social media) and behavioural components (e.g. location patterns). However, the components vary in their capabilities to identify a user, as it is fairly easy to create a fake profile on social media while physical attributes are rather difficult to interfere with (Schukai et al., 2017).

The World Bank (2018) report identifies concepts related to an e-ID system. First, an individual provides an identity, a characteristic that uniquely belongs to the individual, such as a biometric attribute. Next, the fingerprint has to match information contained in a database, which leads to identification, defined as *"the determination of identity and recognition of who a person is; the action or process of determining what a thing is; or the recognition of a thing as being what it is"*. When the identification has been determined the process of authentication follows where an identity claim is verified, defined as *"the process of providing an identity. Occurs when subjects provide appropriate credentials, often as prerequisite to receiving access to resources"*. Finally, the individual providing the identity is verified through verification, defined as "*confirmation and establishment of a link between a claimed identity and the actual, living person presenting the evidence*." (World Bank Group, 2018). Throughout this thesis the definition of e-ID from the World Bank Group is adopted and will serve as a base whenever referring to digital identity or e-ID.

2.3. E-ID USE CASES

The purpose of e-ID is to identify and authenticate an individual. Additionally, that the identified individual receives the service he or she is entitled to. e-ID is important in areas such as e-Government where it allows both businesses and individuals to trust that their data is used in respect and according to legislation such as data protection (eIDAS, 2014; European Commission, 2017; European Commission, 2018). The concept of e-ID can be applied in different industries; however, the goal is to create trust and transparency while interacting digitally. Industries where e-ID have proven beneficial are healthcare, finance and commerce (Halperin & Backhouse, 2008). Identification is prominent in electronic health (eHealth), more precisely in-patient care records system. In this case, identity is a dominant factor where it allows healthcare workers to access patient data from dispersed locations. The challenge is to maintain confidentiality and to have a platform that supports identification processes. Additionally, identification within the financial sector is extremely vital because of fraud and money laundering. Every customer must go through an identity check at the start as well as multiple times during the banking relationship. Financial institutions that are not able to identify their customers may face a fine from the government or even imprisonment, if they do not have strong verification checks implemented. Plus, vast amounts of resources are being spent on ‘know your customer’ (KYC) and ‘customer due diligence’ (CDD) initiatives (Linn, 2005; Halperin & Backhouse., 2008). Other commerce businesses use identity as a marketing tool where special patterns are recognized to tailor advertising or offers to a special target group (Lace, 2005).

Identity plays a different role depending on industries and the nature of the data. As an example, the pressure to verify an identity is more within eHealth than e-governance (Halperin & Backhouse, 2008). Therefore, it is important that an e-ID system includes attributes applicable to all industries where the data management is prioritized. In the Member States of the European Union most business and government sites include a login feature where the user has to access these sites with a username and password. However, such a login is weak, an easy target for hackers and may lead to identity theft. This is especially apparent in relation with the financial industry and phishing. One - and two-methods of authentication is one way to ensure security. In the aforementioned method the user is required to input credentials only the user knows (e.g. password) or something the user has (e.g. card). The two-method authentication requires two elements of both something the user knows and possesses (Kubicek, 2010). The methods are examples of a solution to prevent identity theft. However, there is still an immense number of cases of identity theft. In 2016, 421 billion data records were stolen around the world (Trotman, 2017). Based on the sensitive data that a digital identity holds in industries like eHealth the underlying forces of technology and regulation converge. Therefore, the next section will elaborate the convergence of technology and regulation in the development of e-ID systems.

2.4. INTEROPERABILITY

The concept of interoperability has many definitions and can be applied to various use cases. Interoperability is most often viewed from the perspective of information technology (IT), however, the concept also applies to non-computerized systems (Chen, 2006). Further explained, “the term is often used in terms of technical systems engineering, or alternatively in a broader sense that accounts for social, political, and organizational factors that impact system to system performance” (New World Encyclopaedia, 2018). For the purpose of this paper the definition by Gasser and Palfrey (2012) is followed in that interoperability is "*the art and science of working together*". The research does not focus on scrutinizing systems in detail and, therefore, includes a broader view on interoperability, including the human aspect. According to Paul Miller (2000), "one should actively be engaged in the ongoing process of ensuring that the systems, procedures and culture of an organisation are managed in such a way as to maximise opportunities for exchange and re-use of information, whether internally or externally". Previous research includes interoperability within information and communication technology (ICT) (Palfrey et al, 2007a), enterprises (Chen, 2006), cloud computing (Dillon et al, 2010), internet of things (Gubbi et al, 2013) and health care (Kreps & Neuhauser, 2010). The following table shows an overview of existing interoperability frameworks.

2.4.1. FRAMEWORKS

Table II: Interoperability frameworks.

Source	**Frameworks**	**Concept**
Architecture Working Group (1998)	LISI	Interoperability between information systems
IDEAS Project deliverables (2003)	IDEAS	Interoperability in business, knowledge, application, data and communication layers
ATHENA (2003)	ATHENA	Interoperability on conceptual, applicative and technical levels
NEHTA (2005)	e-Health Interoperability Framework	Interoperability in health organizations in organizational, information and technical aspects
Chen (2006)	Enterprise Interoperability Framework	Interoperability concerns within businesses, processes, services and data

European Commission (2017)	European Interoperability Framework	Interoperability policies, standards and guidelines how organizations should do business

The table above shows existing frameworks on interoperability that focus on the technical aspects. However, none of these frameworks factor in the human aspects that can be significant in evaluating interoperability of a system. The first notable framework was the LISI reference model. The framework investigates levels of information systems interoperability. The IDEAS framework consists of more than one layer. The aim of the framework is to reflect on "that interoperability is achieved on multiple levels: inter-enterprise coordination, business process integration, semantic application integration, syntactical application integration and physical integration" (Chen et al., 2008). Complementary to the IDEAS framework is the ATHENA framework. ATHENA addresses three levels of interoperability conceptual, technical and applicative. The conceptual level identifies research requirements (e.g. modelling concepts) and integrates it with R&D projects. The applicative level integrates experience from the previous level, including technology testing and transfers of knowledge to the next level. Finally, the technology level is used for testing and integrating prototypes (Chen et al., 2008). Furthermore, the enterprise framework consists of interoperability of business, processes, services and data. The goal of an enterprise is to run its businesses; however, data is necessary to provide a service or product. Service interoperability refers to operating various applications by solving conceptual differences and finding connections to various databases. The data is transferred through processes and aims to enable different process to work together. This in turn creates the business of the enterprise. The interoperability of business indicates working in a harmonized way despite business differences such as culture and legislations (Chen, 2006).

The aim of the EU framework is "promoting seamless services and data flows for European public administrations" (European Commission, 2017). The EU framework includes different layers of interoperability, including interoperability governance, integrated public service governance, legal interoperability, organizational interoperability, semantic interoperability and technical interoperability (European Commission, 2017). Additionally, interoperability has been applied to the e-Health sector. The purpose of the e-Health framework is to "document the approaches, policies, information and tools that are shared across the health sector to deliver an interoperable eHealth environment". Furthermore, interoperability is analyzed from organizational, information and technical viewpoints (NEHTA, 2005).

2.4.2. APPROACHES

Based on previous research there are three approaches to developing enterprise interoperability. First, the integrated approach, which creates an interoperability strategy developed through the combination of existing common format for all models. The approach is suitable for designing or implementing a new system. Second, the unified approach, which has been adopted the most in previous research on interoperability. An approach where a common format is developed. It provides a mapping between applications and models and is not bound by an enterprise as the integrated approach. The solution is convenient in situations where a large company needs to interoperate with SMEs and vice versa. Third, the federated approach which refers to a situation when there is no common format. In this case there is no actor that can impose their models or method of work. The federated model is most suitable where companies share their resources and abilities to create a product with a limited duration (Chen, 2006). Palfrey and Gasser (2007a) researched interoperability within the context of information and communication technologies (ICT). Their aim is to understand the concept of interoperability, more precisely how it relates to innovation and different approaches in achieving interoperability. According to the authors, approaches differ depending on circumstances such as the nature of private and public institutions. Furthermore, approaches are determined by different attributes including technical collaboration, transparency for consumers, disclosure of information and open standard initiatives. Based on these attributes, approaches for private actors are unilateral design and IP licensing, technical collaboration and open standards (Palfrey & Gasser, 2007a).

2.4.3. USE CASES

The concept of interoperability is also mentioned in relation to technologies such as cloud computing. Cloud interoperability refers to the linkage both between two clouds as well as between an organization and a cloud. In cloud computing interoperability is essential. First, organizations need to keep their IT functions connected with the company's core competencies within the organization while outsourcing other elements. For instance, interoperability between outsourced cloud services (e.g. HR systems) and on-premise systems (e.g. ERP). Second, it is common that organizations outsource marginal functions to cloud services for the purpose of optimization. The outsourced functions are often different vendors, especially in the case of SMEs. For instance, using Gmail for email services and Salesforce for human resource (HR) services which means that some features (e.g. appointment booking) have to be connected to the HR service. Furthermore, to address the interoperability issue the authors recommend intermediary layer, standardization, open application programming interface (API), software as a service (SaaS) and platform as a service (PaaS) interoperability (Dillon et al, 2010).

Palfrey and Gasser (2007b) define digital ID interoperability as a “constantly shifting interconnection among ID users, ID providers and ID consumers that permits the transmission of digital ID information between them via a secure, privacy-protected channel”. They recommend addressing the concept of interoperability from the perspectives of different stakeholder groups, including individuals (the users), relying parties (provider of services for the users), ID providers and society as a whole (Palfrey & Gasser, 2007b). Furthermore, they describe an appropriate approach for digital ID. The primary ID approach is a non-regulatory (e.g. private actors) single firm approach (e.g. Google) and based open standard initiatives. The approach of open standards is categorized as a way toward achieving a higher level of ICT interoperability (Palfrey & Gasser, 2007a). World Bank Group (2018) report on digital identification, emphasizes the importance of an ID system to be open, interoperable and standardized. An interoperable system creates a platform that delivers efficient services and enables the use of new technology. The interoperability of credentials is important within authentication and for intra/inter-country service delivery (World Bank Group, 2018). The use cases above show the concept being applied to cloud computing and digital identity. However, it is important in many industries such as crisis management. As explained by Avanzi et al. (2017), “it has been shown that crisis management should be directly linked to interoperability issues, allowing an integrated operation of all entities involved during an event”.

2.5. INNOVATION

With increased digitalization, innovation becomes an important factor for success and competitive advantage. New technology has an impact on traditional processes, such as information systems (IS), as it changes the core business technologies (Porter & Millar 1985). Businesses should be aware of external factors such as advancements in technology, including the opportunities and constraints and how it can lead to new organizational products and processes (Swanson, 1988). Innovation is a broad concept, however, the aim in this research is to review the relevant definitions in relation to e-ID. Innovation can be broadly defined as “the first or early use of an idea by one of a set of organization with similar goals “(Daft, 1978). Furthermore, innovation can be distinguished between product and process innovation. Product innovation refers to “the introduction of new products or services that shift or expand an organization’s domain” while process innovation refers to “the introduction of new methods, procedures or responsibilities within existing domains”. As a result, product innovation follows a shift within company’s resource allocation patterns while process innovation leads to shift in individual task behaviour (Zmud, 1982).

According to Swanson (1994) there are three types of IS innovation: I, II and III. Type I innovation is described as a “process innovation restricted to the IS core”, where other aspects of the business are in most cases indirectly affected. The first type of innovation can be classified into two subtypes. Type I(a) innovation where the focus is on IS administration and Type I(b) the focus is on technical tasks. Type II innovation "applies IS products and services to the administrative core of the host organization business". In Type II, the core production of the organization's products and services is not directly affected, rather, leading to changes in the internal IS work process. Type III innovation "integrates IS products and services with core business technology, and typically impacts upon general business administration as well". In the case of type III, the whole organization may be affected. Type III can be classified into three sub-categories. Type III(a) innovation which is centred on the business's core work process, type III(b) innovation which extends to basic business products and services and type III(c) which provides the integration or effective coordination of the business including suppliers, distributors or customers. Type I innovation focuses on IS process innovation while Type II and III involve IS products in the service of basic business processes and products (Swanson, 1994).

Yoo et al. (2010) define digital innovation as "carrying out of new combination of digital and physical components to produce novel products". Furthermore, they identify three characteristics of digital innovation; the re-programmability, the homogenization of data and the self-referential nature of digital technology. First, digital innovation is re-programmable in a way that it can be separated from the "physical embodiment that holds it". Additionally, allowing the device to execute several functions such as video editing and web browsing. The re-programmability requires manipulation of the data to allow for adaptability. Second, homogenization of data, where digital data can be combined in various ways both coupled with other content as well as combined with other data to combine new services. Third, self-reference, meaning the use of digital innovation can enable other digital innovations. Such as, ease of access to computers leading to increased usage of digital tools (Yoo et al., 2010). Palfrey et al. (2007b) introduce digital ID innovation. The innovation is defined as "the process of developing and introducing new elements into products and services" (Palfrey et al., 2007b). The definition can be interpreted in both a closed and an open sense. In a closed sense this refers to the innovation to be found in product updates or new feature releases while innovation. In an open sense also includes new developments by others, such as, users or third-party programmers. Innovation can appear in technology and in business models within the digital ID space (Palfrey et al., 2007b).

2.5.1. INNOVATION NETWORKS

Innovation occurs when it is shared between several actors in a socio-technical network. Such a network consists of a flow of "fragile and uncertain knowledge translations where ambiguous, conflicting ideas, representations and material artefacts become assembled through the interaction of diverse actors into new knowledge combinations of resources" (Lyytinen et al., 2015). The authors define four types of innovation networks: the project innovation network, the clan network, the federated network and the anarchic network. The networks are distinguished depending on "heterogeneity of operant resources" and "distribution on coordination and control via operand resources". The project innovation network is centralized and consists of homogeneous actors. The actors share similar perspectives and work with standardized tools. An example of such a network is a capability maturity model. The clan network is distributed and consists of homogeneous actors. The actors within the network share a common interest in a specific type of product, however, do not operate under a hierarchical control structure. An open source community is an example of a clan network. A federated innovation network is a centralized network, consisting of heterogeneous actors. The goal is to create a product where one entity, within the network, guides the process. An example of a federated network is large manufacturing work such as the aerospace. Finally, the anarchic innovation network is distributed and consists of heterogeneous resources. The network is the most complex of all four consisting of several teams working on a product or service in turbulent markets such as a new mobile service (Lyytinen et al., 2015). The following table shows an overview of the four innovation networks.

Table III: Four types of innovation networks (Lyytinen et al., 2015)

Heterogeneity of operant resources	Distribution of coordination and control via operand resources	
	Centralized	Distributed
Homogeneous	Project innovation network (e.g. capability maturity model)	Clan innovation network (e.g. open source community)
Heterogeneous	Federated innovation network (e.g. aerospace)	Anarchic innovation network (e.g. new mobile services)

Another type of network, horizontal networks, is focused on software projects. Horizontal innovation consists of a network of actors that are open to innovation. The network is related to the federated innovation network described above consisting of heterogeneous actors. The actors benefit from the work of others which means that they do not have to create a product or a service from scratch. The goal of the innovation network is to create a product or a service that benefits all. Actors within a horizontal innovation network include for instance development, production, distribution and consumption teams. The network flourishes when "at least some of the actors have the incentive to innovative", "at least some actors are willing to share information which enables others to reproduce their innovations" and "the actors' production is compatible with commercial products and distribution" (von Hippel, 2007). When the three conditions are in place, the network will flourish and in turn lead to an innovative product made by several actors collaborating across industries or interests (von Hippel, 2017).

2.6. E-ID TRENDS IN THE REAL WORLD

As the earlier sections highlight the forces of technology and regulation are vital in the development of e-ID. Innovation within e-ID is becoming more apparent with increased interoperability, both on a technical and human level where actors are collaborating within government, businesses and society. This results in interoperable e-ID innovations. In the past years several trends have emerged. One of the trends is an OpenID infrastructure, where the user is the owner of the data and the systems that represent his or her identity. For instance, in 2008, the Italian Ministry of Interior (a government agency of Italy) opened their national e-ID file system which until then had been confidential. The service had been restricted to a single platform and one web browser. As a result, OpenID infrastructure enabled interoperability between national e-ID and online businesses within the private sector (Arora, 2008).

Estonia is a leading example of a government implementing an interoperable e-ID system. In March 2018, Estonia received the Government Leadership Award for digitally transforming their government services and for having 95% of their services accessible through a mobile ID (e-Estonia, 2018). Estonia's national e-ID is an identity card available for citizens and non-citizens. The identity is powered on the Blockchain technology and allows the user to connect to public and private services, including e-voting and travelling within the EU without carrying a passport. The ID is open for developers to build other services to extend the e-ID platform even further (Hammersley, 2017; Shen, 2016). All of the functions are connected to a database called the X-Road. The X-Road has gained trust among citizens and the service has expanded to other countries such as Finland. Their digital identity puts the individual in control over their own data by allowing them, for instance, to choose who can access their medical records. The X-Road creates a joint digital identity on a shared platform. Moreover, the goal of e-Estonia is to increase digital innovation within public services and society. Furthermore, creating common procedures and standards to build a secure and interoperable system for bottom-up innovation (Anthes, 2015).

Another innovative e-ID system is Aadhaar. The identity was issued by the government of India in 2016 with the objective of providing its residents a robust, easy and cost-effective way of identification. The result was a Unique Identification number (UID), a 12-digit number called Aadhaar. The residents of India are verified using the Aadhaar authentication number online at any time. Also, accessing services such as opening a bank account and applying for a driving license (UIDAI, 2018a; UIDAI, 2018b). The technology behind the identity consists of an UIDAI (Unique Identification Authority of India) database for verification. The identity is built on biometrics and does not require information such as religion or geography. Additionally, it uses open source technologies, to further develop applications to address scalability (UIDAI, 2018c). In early 2018, 1,2 billion people have an Aadhaar number, which represents about 99% of India's adult population (Gemalto, 2018c).

In 2008, the European Union founded a project called STORK. The goal of the project was to implement "an EU wide interoperable system for recognition of e-ID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State" (Arora, 2008). The project has led to the eIDAS regulation which will be mandatory from September 2018. The regulation is part of the Digital Single Market and will ensure a cross-border mutual recognition of e-ID across borders (European Commission, 2017). The EU values the input from the private sector in creating beneficial regulations where the public and private sector collaborate. According to a conference held in 2014, the private sector stressed the need for a cross-border e-ID. One of the results of the conference was that private companies could benefit from integrating e-ID in their business models and thereby enabling innovation (European Commission, 2015).

A trend within e-ID is a self-sovereign identity which is built on the Blockchain. This type of identity allows a person to have total control over his or her personal data, can limit and control the information that is shared (Milanovic, 2017). According to Clippinger (2018), third parties are the source of creation of an individual's identity credentials, such as social media sites, the government or banks. A self-sovereign identity on the Blockchain needs to follow legal rules and policies. Additionally, it has to have the trust of the people to adopt the identity. Therefore, self-sovereign identity must be a collaboration between different actors such as governments, private companies, non-profits and individuals (Milanovic, 2017).

There are not only governments and regulators who acknowledge the importance of interoperability. In 2012, the Fast Identity Online (FIDO) alliance was established. The goal of the alliance is to address the lack of interoperability within authentication. The alliance is user-focused and addresses the problems that users face when having to create and remember many usernames and password for different logins. Furthermore, the alliance introduces two frameworks that make authentication simple: Universal Authentication Framework (UAF) and Universal Second Factor (U2F). The two frameworks introduce protocols where authentication is performed on a user's device (FIDO Alliance, 2018). Other alliance within e-ID is ID2020. Their aim is to solve the problem of lack of identification through technology. Meeting this challenge, they have developed an interoperability framework that connects actors within non-profit organizations, governments and the private sector. The framework is based on open standards and open API, making room for innovation and development within the ecosystem (ID2020, 2018).

2.7. SUMMARY

From the examples above there is a growing interest in an interoperable e-ID solution. However, as mentioned, underlying forces such as technology, regulations and cultural differences have to be taken into consideration. As evident from the sections above, identification schemes date back to ancient times. However, schemes of identifying have changed due to the change in requirements and advancements in technology. The literature highlights the evolution of identity from Identity 1.0 to Identity 2.0 and eventually Identity 3.0. Additionally, there have been different meanings and definitions tied to e-ID, however, in sum they mean the same that an electronic identity is a tool to access digital services by proving your identity in a safe and secure way. The purpose of an e-ID system is to identify and authenticate an individual, therefore, it opens up for various applicability in this increasingly digital world. Identification is prominent in electronic health (eHealth) allowing healthcare workers to access patient data in a secure and verified way. From the research it is prominent that resources are being allocated to implement KYC and CDD initiatives and e-ID can be considered as a vital tool in this endeavour.

However, from the above-mentioned literature there has been a lack of focus on e-ID in connection with interoperability and innovation. The aforementioned section highlighted the benefits of interoperability as evident in it applicability in various industries. However, the focus of interoperability has been researched to uncover its potential purely through a technical perspective. Furthermore, it is evident that the concept has been applied to the field of e-ID, where the EU introduced the EIF framework and the eIDAS regulation that allows citizens and businesses to access public service in other member states. Furthermore, research highlights innovation networks which allow actors to create a product or a service that benefits all by sharing ideas and expertise which can be applied to e-ID. There are examples of success stories such as Estonia who is a leading example of a government implementing an interoperable e-ID system. Other include India’s Aadhaar that uses open source technologies, to further develop applications to address scalability. Another trend within e-ID is a self-sovereign identity which is built on the Blockchain. This type of identity allows an individual to have total control over his or her personal data, can limit and control the information that is shared. Therefore, there is a growing need to research e-ID in connection with interoperability and innovation by accounting for technology, regulation and cultural differences.

3. THEORETICAL FRAMEWORK

In this section of the paper the theoretical framework is introduced and explained based on which the data collected will be analysed. The framework will also be used as the lens through which we investigate and will continue to act as a filter to answer the research question. For the purpose of this paper the research of interoperability was chosen. From previous research as highlighted in the literature review, interoperability is a concept that has strong ties to engineering and systems integration. It focuses on standardization and integration through technology and data. Albeit this, our approach toward interoperability can be seen as a combination of technical and organizational issues. Gasser and Palfrey (2012) have conducted research on interoperability and how it can lead to innovation depending on the context. This is directly related to the research we aim to conduct and therefore, look at interoperability as a driver of innovation in the context of an electronic identification system. Below, we explain the theory of interoperability put forward by previous mentioned authors. We have chosen to follow their footsteps as we believe that interoperability holds value in understanding both technical and organizational issues.

3.1. THE THEORY OF INTEROPERABILITY

For the purpose of this research authors Urs Gasser and John Palfrey have been chosen and their work on interoperability. The intention is to understand how interoperability can be a driver to innovation. The authors have chosen based on their findings that link interoperability and innovation which is what this study aims to unveil. It will build upon their view that the concept of interoperability exists not only in the realm of technology but can also be used to explain interconnections in other fields. The authors make the point that interoperability has a negative and positive side though the positive outweighs the negative. One of the main contributions of interoperability when achieved to an appropriate level preserves diversity but allows for alignment of common ground.

There is still no single definition of interoperability. Many authors have tried to define the term such as the share and flow of information across systems. However, we adopt the simplistic definition by Gasser & Palfrey (2012) that interoperability is, "*the art and science of working together*". It is a more holistic approach that can be applicable to many situations depending on the context. It allows one to look at several issues caused by lack of interoperability.

When addressing interoperability, one must consider that the need to be interconnected and interdependent is an ongoing challenge and it has allowed us to remain global. The questions one should ask when thinking of interoperability are:

1. How much information should be shared?
2. What are the design challenges with system interoperability?
3. What degree/level of interoperability does the system need to have?
4. How do we theoretically and practically get to interoperability?

The authors work builds upon the premise that "interoperability sounds like a technical concept. It evokes gears that interlock with one another or massive data flows across corporate firewalls. But it turns out that the human aspects of interoperability are often just as, and perhaps, even more important than the technological" (Gasser & Palfrey, 2012). They have identified different interop layers in their book *Interop: The promise and perils of highly interconnected systems*. There layers of interoperability are namely, data, technology, human and institutional layers. We will further explain each layer as the applicability of each one is important in understanding the integration of systems and the role of individuals. They argue that the institutional and human layers are just as important as the technology and data layers. It is a combination of the four that is required based on the situation and context.

3.1.1. TECHNOLOGY & DATA LAYERS

Consumers in an increasingly digitized economy expect technological systems to work together seamlessly. When they experience trouble with a system, the lock-in effect has to be strong else the customer will easily switch to another system. Palfrey and Gasser successfully describe the modern consumer as "we simply want systems to work together when we want them to and to not work together when we do not" (Palfrey & Gasser, 2012). The technology layer deals with the compatibility of different systems to work together to achieve data exchange at the highest level. In some cases, different systems work well together and there is not much trouble for the consumer in using different types of systems. For instance, taking a photo with a phone, sending the photo via Gmail, a friend receiving the photo on Office mail and finally sharing the photo on Facebook. Though the trouble for the consumer is not high the magic behind the process is the invisible links that make this happen. Therefore, the technology and data layers are highly connected (Palfrey & Gasser, 2012).

The data layer consists of format and data protocols. Interoperability at the data layer depends on the structure and standardization of the data. As such, two different systems have to be able to communicate by exchanging data. Interoperability occurs when technologies work together and the data they exchange are rendered useful on the other end of the transaction. However, even though there are many benefits in creating interoperability through technology and data it also involves problems. First, the interest of businesses and consumers are often not aligned, for instance, the free flow of sensitive information. Second, not all systems are designed to be interoperable, some companies choose not to be interoperable to create lock-in. The technology and data layers are highly important in creating interoperability. As the authors argue "without interoperability at the technology and data layers, interoperability at the highest layers in our model - the human and institutional layers is often impossible". However, as mentioned, all of the layers are dependent on each other to create a fully interoperable system. Therefore, interoperability requires work and knowledge on the human layer (Palfrey & Gasser, 2012).

3.1.2. HUMAN & INSTITUTIONAL LAYERS

The human layer of interoperability allows individuals from different organizations and firms to work together across a network by effective communication. A certain common goal that needs to be reached requires cooperation between individuals. The user who needs to get access to a system and the companies providing the access. They need to work together and interconnect to reach their shared goal. Individuals rely on technology to communicate and work efficiently, if they are able to work together and get the job done then it is a proof that the technology used is effective. As the authors outline "language is the clearest way to demonstrate the need for interoperability at the human layer" (Gasser & Palfrey, 2012). Having stated that, the issue of language can be further broken down into semantic, syntactic and lexical. When information is shared across and between systems there is a need to comprehend the information. To understand and interpret the information as there are different levels of meaning. It becomes more complex as businesses work in an international market where the barriers to interoperability become higher (Gasser & Palfrey, 2012).

The Institutional layer of interoperability allows different businesses to work together by laying down the guidelines and procedures. For different businesses to work together there needs to be alignment at the institutional layer. For this alignment the rules, safety standards, business processes and communication protocols that the businesses follow need to be adjusted in order to reach a common goal by working together. Through standardization of rules and protocols businesses can cooperate and integrate efficiently. For example, open standards that allow for innovation and sharing of expertise. Further elaborated by the authors "rules make up a central element of what economist and legal scholars refer to as institutions, one of the reasons we refer to these layers as institutional" (Gasser & Palfrey, 2012).

A combination of the four different interoperability layers data, technology, institutional and human can create highly integrated and complex systems. In certain industries a combination of the layers of interoperability can even save lives. However, due to this high level of integration and complexity these systems work efficiently in one setting but might not work efficiently in another. As stated by the authors "how we work together as humans, often relying upon technological tools to communicate, can determine whether the most seamlessly interoperable technologies prove effective for the given task" (Gasser & Palfrey, 2012). Due to advancement in technology and innovation at an incredibly high pace, these systems need to incorporate flexibility and adaptability. Therefore, the next section covers interoperability and innovation.

3.2. INNOVATION

One of many potential benefits of interoperability is innovation. With increased digitization web innovation has been prominent such as in relation to social media and API. As stated by the aforementioned authors "innovation in web services has been central to the evolution of the web over the past decade. This innovation derives in large part from the availability of different data sources and functionalities obtained via multiple open APIs". As companies open up their platforms through open APIs, it allows others to build upon the open system which could potentially lead to innovation (Palfrey & Gasser, 2012).

Furthermore, innovation can result from interoperability in one or more than one layer. As such technical interoperability enables innovation within the human and institution layers. An example of how interoperability within the technology and data layers has an impact on the human and institution layer is the earthquake in Haiti in 2010. After the disaster the central platform Ushahidi was created. It allowed individuals and businesses, who are on the ground in a crisis, to access information from many data sources, in one platform. The data came from text messages and social media posts. The platform combines different technical components in an innovative way. Consequently, the platform enabled other actors within society to access updates in one place and receive reports after the crisis to increase crisis management efforts. Although, interoperability fosters innovation it is important to note that it might not enable innovation directly, rather it can help drive innovative initiatives on the market. As a result, a small-step innovation which leads to new ways of combining components or system. Consequently, development of new product or services as well as improved system efficiencies (Gasser and Palfrey, 2012).

The authors further state that one of the benefits of interoperability are the resulting systemic efficiencies. Most interoperability benefits have been targeted toward the customer but system efficiencies can benefit businesses in consolidating their processes and practices. Systemic efficiencies can be explained as the improvement and optimization in certain business processes that help achieve a certain end task in a more effective manner. To gain system efficiencies, consider a department in a firm to be a network of different actors (the employees of that department) conducting different actions to eventually a common goal. The current processes of identifying and validating customers is done by manually checking each data point against the other. However, if a new process were to be implemented where a system would do the checking then the whole process is optimized and smoothened out (Palfrey & Gasser, 2012).

Moreover, benefits can be classified into marginal and radical change based on the transformation interoperability will achieve. Marginal changes can be referred to as changes that are small in size, less important and more common. They take place when there already exists a certain degree of interoperability but a change in the degree of interoperability improves a certain process but does not change it entirely. While radical changes are large in size, more important and not that common. It can be explained as jumping from one use of a system to a whole new use for that system. Radical change can be developed when there are no interoperable components between systems and through manipulation make them interoperable. “This phenomenon of radical improvements has a great deal to do with increasing levels of data generation and connection in society at large” (Gasser & Palfrey, 2012).

Based on the interoperability theory an initial framework was made. The research design will be based on this model as well as the findings of the research. The illustration below is based on the theory of interoperability applied to an e-ID system. When developing a system all four layers need to be accounted for. This model is the theoretical framework against which the results will be analysed.

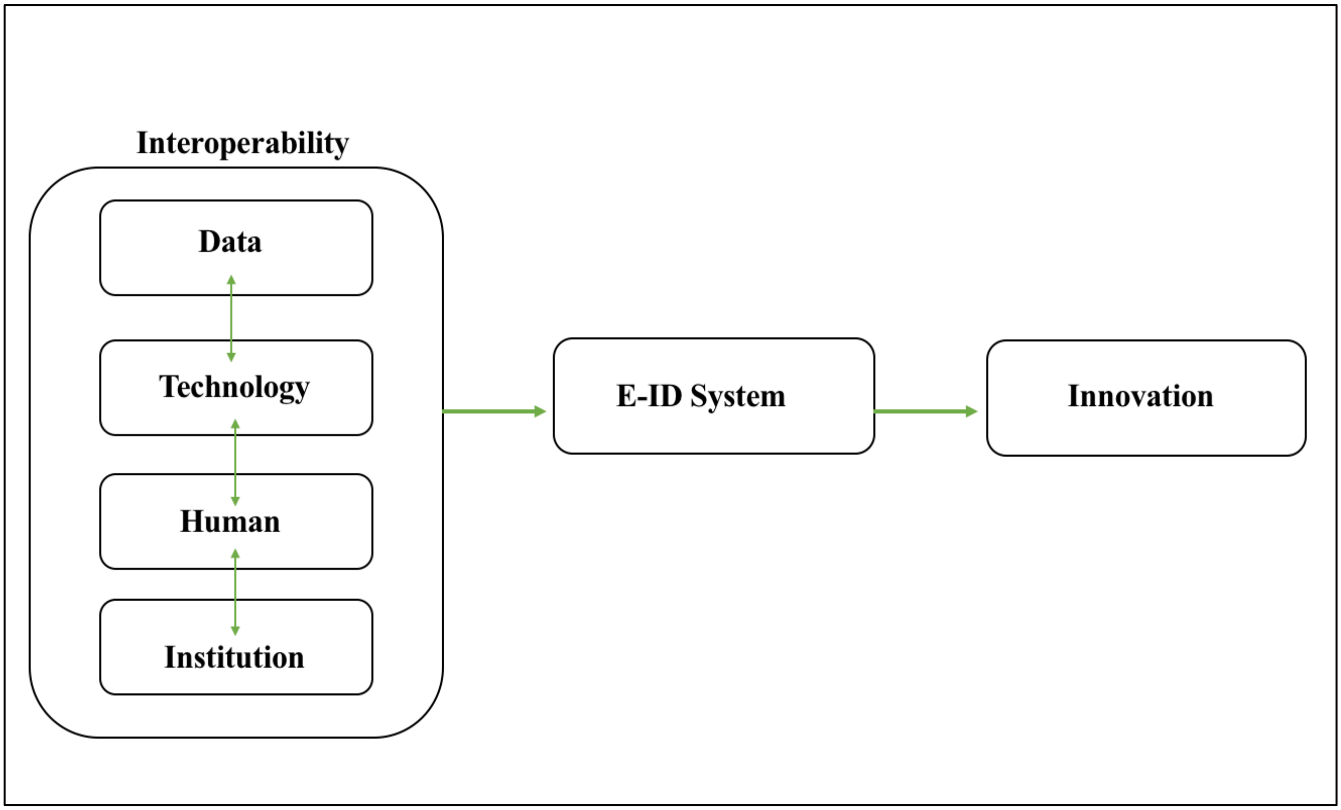


Illustration I: Initial framework.

4. METHOD

This section describes the research process which will include how it was designed and executed. It will also include the methodological choices that were used as a guide throughout the research to help create more structure and answer the research question. In the following section the research design, the data collection process, the users in our field study also known as the actors, and the approach that was used in analysing the data is introduced. The research is not without limitations and there exists alternative methods in answering the research question, therefore, reflections on alternative methods are included in the discussion section of the paper. The nature of this research is qualitative "... as the focus will not be on trying to estimate things about a population, but in trying to understand or relate the data to theory or ideas" (Greener, 2008). Below is an illustration of the methodology which will be explained in detail in the sections to come.

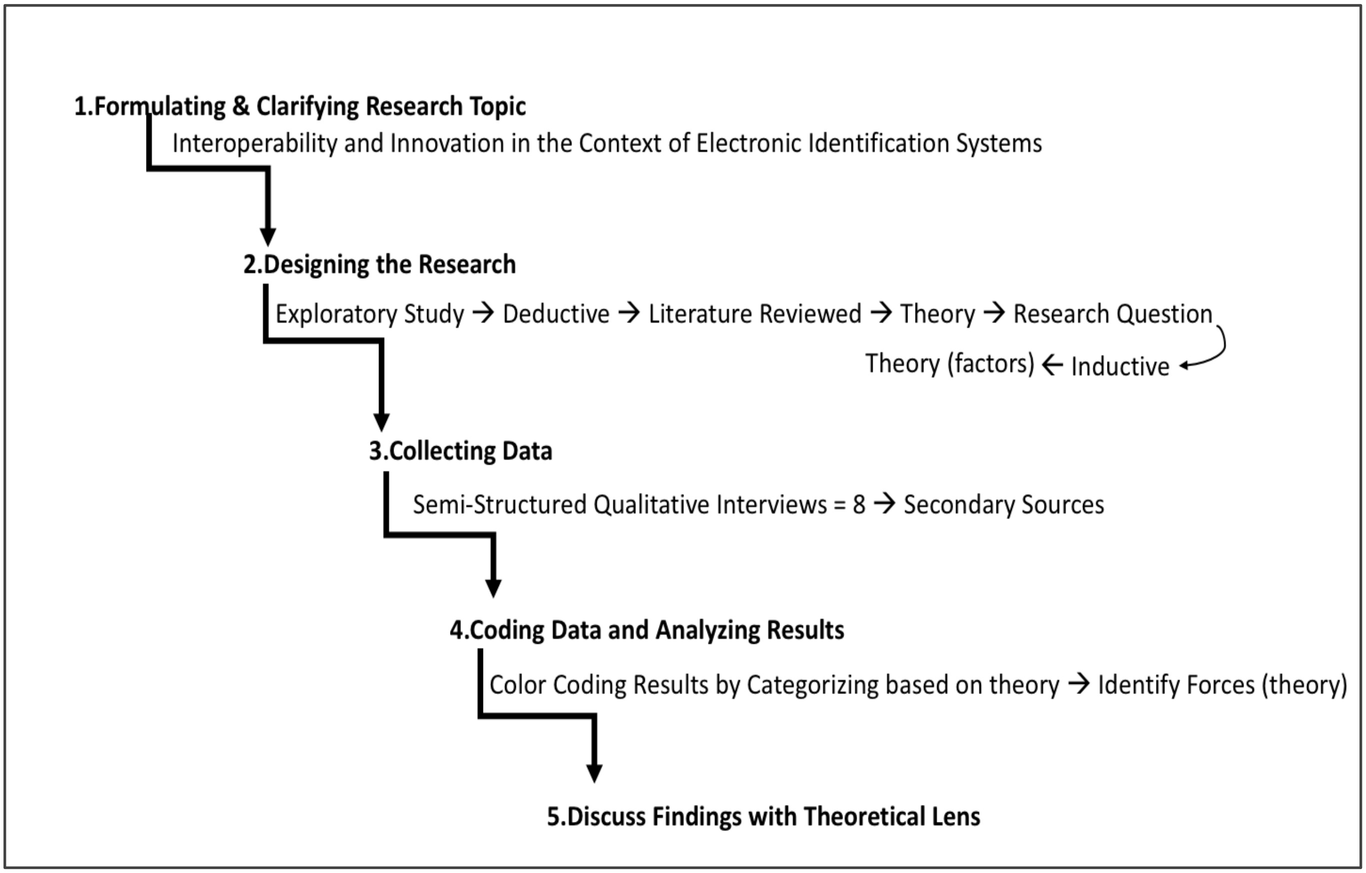

1.Formulating & Clarifying Research Topic
Interoperability and Innovation in the Context of Electronic Identification Systems
2.Designing the Research
Exploratory Study → Deductive → Literature Reviewed → Theory → Research Question
Theory (factors) ← Inductive
3.Collecting Data
Semi-Structured Qualitative Interviews = 8 → Secondary Sources
4.Coding Data and Analyzing Results
Color Coding Results by Categorizing based on theory → Identify Forces (theory)
5.Discuss Findings with Theoretical Lens

Illustration II: Research design.

As will be mentioned in the sections to come, an exploratory field study was chosen for the research. The selected companies belong to the private sector, more specifically to the organization category of start-ups. The actors selected were MEDEI Aps, Calcabis, CMP Company, and, CoinsIntel. Additionally, as the topic is structured around the topic of e-ID the Danish Agency of Digitisation was interviewed which opened up to a broad view on the current and future plans of the national Danish e-ID (MitID). Start-ups were chosen for the research due to their openness toward new technology and innovation. In describing our research design, we follow the research onion by Saunders et al. (2012).

4.1. PHILOSOPHY AND APPROACH

The research philosophy chosen belongs to the interpretive research paradigm. “An interpretive paradigm uses a qualitative research method such as discourse analysis, unstructured interviews to investigate perceptions and constructions of reality by “actors” in organizations, i.e. employees, managers, shareholders etc.” (Greener, 2008). It is important to state and explain the philosophy as the research is qualitative in nature, based on which we as researchers understand things and consider certain data more important and relevant in answering the research question.

From an ontological point of view the researchers are subjectivist. For example, and what is directly relevant is that of organizational culture and its subsequent development, “...the subjectivist view would be that culture is something that the organization ‘is’ as a result as a process of continuing social enactment” (Saunders et al., 2012). Furthermore, following the path that concepts like organizational culture where individuals need to interact and that this action cannot be manipulated it is something that is inherently built through the values and beliefs of the employees. The norms and values that belong to an organization and “that culture is something that is created and re-created through a complex array of phenomena which include social interactions and physical factors such as office layout to which individuals attach certain meanings, rituals and myths” (Saunders et al., 2012).

From an epistemological point of view, we identify ourselves as that of the interpretivist. Acceptable knowledge has to be interpreted in terms of differences between social actors and their social roles in everyday life. We identify with the “feelings researcher, who is concerned with the feelings and attitudes of the workers towards their managers in that same manufacturing process” (Saunders et al., 2012). The case that we are researching is complex as it seeks to understand the subjective meanings associated with a more objective concept. Our understanding of what constitutes acceptable knowledge is therefore bound by subjective meanings with a focus on the details of the situation as well as the reality behind these details and that subjective meanings motivate actions.

Although, it is recommended to follow either a deductive or an inductive approach, however "not only is it perfectly possible to combine deduction and induction within the same piece of research, but also in our experience it is often advantageous to do so" (Saunders et al., 2012). Therefore, for the purpose of this research deductive and inductive approaches are combined. We believe that though separately these methods have advantages and disadvantages through a plausible combination we are able to use the advantages of both. The research approach began with a deductive approach where we highlighted the existing literature and then selected a theoretical framework this is evident from the previous chapters. Based on this we were able to search for a relationship between the 'interoperability layers and innovation'. We then proceeded with an inductive approach in an attempt to find contributions to the literature. Once the relationship was established we then sought out to understand this relationship and to explore and discuss implications of the current literature. To do this we explored the resulting factors that foster innovation in the context of e-ID by interpreting the interviews. These factors are the contribution we make by taking the literature one step further in the understanding of interoperability and e-ID.

4.2. RESEARCH DESIGN

The aim of this research is to conduct an exploratory field study in the private sector. More specifically, focusing on how start-ups utilize e-ID and the need for more innovative solutions to safely and securely conduct businesses in a digitalized world. An exploratory study was chosen because it aims to find "what is happening; to seek new insights; to ask questions and asses to phenomena in a new light" (Robson, 2002). Additionally, one of the ways to conduct an exploratory research is to search the literature and interview 'experts' in the subject. This research shows a snapshot in time of what is happening in the private sector, with regards to e-ID systems and interoperability. Hence, interviewing different actors within the field, an exploratory research is a natural choice. A field study was chosen to gain knowledge on how private firms are using e-ID currently and their thoughts on an interoperable system. In this paper, first the literature was reviewed, a theory chosen and a research question developed. Next, the theory was tested by conducting a qualitative research. The outcome was then examined and modified in the light of the findings. The study is cross-sectional where it shows a "particular phenomena at a particular time" (Saunders et al., 2012). As the concept of e-ID is in an early development, the outcome of the research shows the business perspective at this time, however, the results might not be the same if the study is replicated in coming years. One actor within the public sector and four actors in the private sector were chosen for the research.

4.3. DATA COLLECTION

Following the above-mentioned research design and approach the research question was identified. The research question is mentioned here to shed light on the interview guide as the questions were created with the research question as the end goal. This research question will continue to be the filter on all sections as we work to answer it. It is one of the most important things we seek to learn through the completion of this research.

How does interoperability foster innovation through electronic identification (e-ID) systems?

Interestingly enough data collection through qualitative interviews is not new “in one sense, interviews have a very long history in human culture. In ancient Greece, Thucydides interviewed participants from the Peloponnesian Wars to write the history of the wars, and Socrates developed philosophical knowledge through dialogues with his Sophist opponents.” (Brinkmann, 2014). The data collection for the research was done by conducting semi-structured interviews with different actors that could contribute to the field of e-ID. A qualitative method was chosen for the research to explore e-ID and interoperability from the view of the private sector. Since the characteristics of a qualitative method is “to gain a rich data on a subject in as real as is possible” (Robson, 2002).

The data collection was conducted through primary sources which include qualitative semi-structured interviews. The interviews included pre-determined questions that allowed for a certain level of flexibility depending on the response of the actor. However, the questions varied depending on the actors interviewed. Follow-up questions were added depending on the flow of the interview and to emphasize specific topics which will be depicted in the interview guide in the appendix. Self-selection sampling was chosen in selecting the actors as “self-selection sampling occurs when you allow each case, usually individuals, to identify their desire to take part in the research” (Saunders et al. 2012). The knowledge gaining process is viewed as a collaboration and partnership with those interviewed and therefore self-selection sampling was chosen. The individuals were contacted via their emails that were provided on the website of the co-working spaces their offices are located in. This also provided us with a short introduction to the company before contacting them. The shared mutual interest in the topic on the part of the interviewees contributed to the research process as they were interested in sharing their ideas.

Two separate interview guides were created before conducting the interviews. The first guide was framed for an interview with an actor within the government. The aim of the interview was to gain a better knowledge of e-ID, in this case the Danish national e-ID (MitID). Second, the same interview guide was then tailored to the four actors in the private sector. The goal of the interviews was to understand how e-ID is currently being used by the companies, both internally and externally. Additionally, to understand challenges within identification and authentication in the private sector and potential benefits of increased interoperability. After the first round of interviews, new knowledge was gained on the topic. Therefore, round two of the interview process required a new interview guide focused on a potential solution to the problems mentioned by the actors in the first round. The questions in round two were targeted toward a potential solution built on the underlying factors identified and how it would benefit the actors.

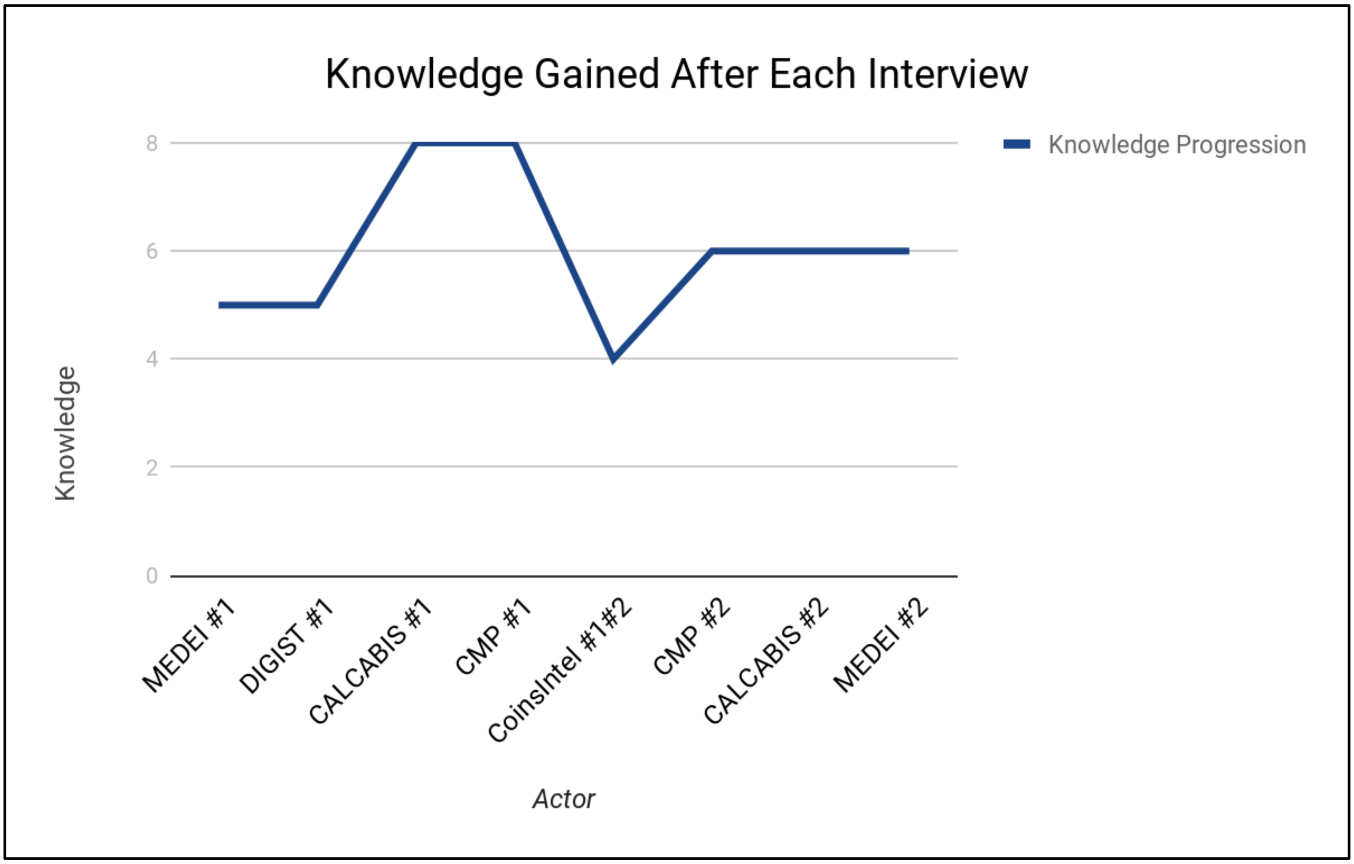
Moreover, the questions that formulate the interview guide were based on the topics of interoperability, innovation and e-ID. Before the interview, the actors received a copy of the concepts and general questions that would be discussed. The purpose of this was to give them time to prepare and introduce them to the topic to be discussed. The interview guide was based on Kvale's (1996; quoted in Bryman & Bell, 2007) suggestion on different kinds of questions. Kvale suggests nine different kinds of questions, introducing, follow-up, probing, specifying, direct, indirect, structuring, silence, and, interpreting questions (Bryman & Bell, 2007). For the purpose of this research a mix of the above questions were used. At the interview, the actor was asked general information such as name, age, gender and specific information such as position in company as suggest by Bryman & Bell (2007). The interview guide is divided into three different sets and each set is further categorized. The two sets were needed based on the fact that each actor was interviewed twice. The first round was focused on finding a problem or challenge and the second round focused on solution-based insight generation. Additionally, we conducted an interview with an actor from the Agency of Digitisation Denmark, to get an understanding from the perspective of the public sector and to learn more about the existing solution, NemID.

The following table shows an overview of the actors interviewed, as well as the date, duration and location where the interviews were conducted. Note, all locations mentioned are the offices or home offices of the actors' interviewed.

Table IV: Data collection.

Actor	Who?	When?	How long?	Where?
MEDEI Round 1	Jon Ingi Bergsteinsson	14.02.2018	33:16	Rainmaking Loft
Agency of Digitalization	Mogens Rom Andersen	06.03.2018	29:29	Landgreven
Calcabis Round 1	Kasper Wodstrup Rost	15.03.2018	51:20	CPH FinTech Lab
CMP Company Round 1	Dan Christensen	17.03.2018	40:51	Fredericiagade
CoinsIntel Round 1&2	Tomas Mikula	28.03.2018	45:38	Holmbladsgade
CMP Company Round 2	Dan Christensen	25.03.2018	50:23	Fredericiagade
Calcabis Round 2	Kasper Wodstrup Rost	13.04.2018	33:13	CPH FinTech lab
MEDEI Round 2	Jon Ingi Bergsteinsson	19.04.2018	49:34	Rainmaking Loft

All of the interviews were recorded with the consent from the actors. Furthermore, the interviews took place within the time of two months and were from 30 minutes up to one-hour long. After the data collection the records were transcribed and further processed. The transcription was done in verbatim by converting spoken word into text, word for word. This was done so that it would be possible to capture the emotion of the words spoken.



Graph I: Knowledge Progression Graph. Data Saturation.

The image above shows a graphical representation of the interviews and the knowledge gained. The sample size was eight interviews in sum. The aim of this representation is to show the knowledge gained with each interview. The measurement also enabled us to effectively decide on concluding with the interviews once we felt we had obtained sufficient information. When no new knowledge was gained and saturation was reached a strategic decision was made to end the data collection through interviews while also being realistic about the limitations of time and complexity. On reflection, the graphical representation can be considered paradoxical. As the graph is, it is indicative of saturation. However, on completion of the analysis the graph represents a paradox. On analysing the data, the researchers learned more and with additional interviews the data collection process could have been restructured to fit the new knowledge. The graph would look different with additional interviews where more knowledge could have been gained. This can be considered a limitation and will be included in the limitations section of this paper as we are aware that no research is without limitations. Furthermore, our choice to conclude data collection still holds valid as the research process needs to account for deadlines involved. Additionally, this research is aimed at providing a step in the understanding of interoperability when applied to e-ID and as such does not compare the views of the interviews in an ongoing state.

4.4. DATA ANALYSIS

The data analysis process involved summarizing, coding, categorizing and unitizing the data. A deductive approach was followed for the initial part of the analysis where the data was categorized by choosing the main components based on the theory of interoperability. The first objective was to identify a relationship between interoperability and innovation. This was done by first, summarizing the main findings in each interview. The process of summarizing involved shortening statements from the transcript (Kvale, 1996; quoted in Sanders, 2012). The summaries showed patterns in the data. Second, the qualitative interviews were coded to sort through the data and to provide structure. By coding we were able to draw upon and understand the underlying links in the data. This further contributes to the analysis and discussion sections where we were able to draw out conclusions based on the data and theory. Third, by categorizing the quotes against the main concepts of the paper it contributed to the first step of the analysis process. The last step was to unitize the data where the units of data from each interview were combined. Through this process of analysis, we were able to identify the link between interoperability and innovation in the context of e-ID.

The below matrix representation, gives a simplistic description on how the analysis will build up. In the analysis section we describe each interoperability layer and have identified a quote that plausibly explains the relationship between the quote and the corresponding layer. We then link interoperability to innovation in the same manner of matching a quote to the underlying theory. Below is an example of matching the actor's comments to the theoretical concepts. The 'x' indicates which actors mentioned the corresponding concepts in the interviews.

Table V: Data analysis.

Concept	**MEDEI**	**CALCABIS**	**CMP**	**CoinsIntel**
Interoperability (General)	x	x	x	x
Data	x	x	x	x
Technology	x	x	x	x

Human	x		x	
Institution	x		x	
Innovation	x	x	x	x

On fulfilling the first objective of identifying the link between interoperability and innovation the next objective was sought after which was to investigate how interoperability fosters innovation. This required an inductive approach were certain factors were identified from the previously analysed data. The factors identified foster innovation within e-ID systems and also contributed to answering the research question. The next section explains the companies that the actors interviewed work in. This also includes the positions they hold which gives context to their opinions as it shows where they are coming from based on their industries.

4.5. CASE SETTING

The reason for selecting the private sector as the focal point in the research is twofold. First, the newness of the topic and the willingness of start-ups to share information played a large part in the selection process. Second, as digital identification is a relatively new area in relation to start-ups and there does not exist vast amounts of research on this perspective. Below, we provide an overview of the companies that cooperated with us and the varying industries that they work in. All the companies except for the Agency of Digitisation belong to the private sector and can be classified as start-ups. Mentioned in the previous section all the interviews were held at the offices of the interviewed.

Agency of Digitisation

"The Agency for Digitisation is an agency within the Ministry of Finance and was established in 2011 to be in charge of the government's digitization policies. With the aim of renewing the Danish welfare, the agency is responsible for the implementation of the government's digital ambitions and the use of digital welfare technology in the public sector" (Agency of Digitisation, 2018). The main reason for the interview was to gain knowledge on national e-IDs, in this case the development of the Danish identification system, from NemID to MitID. Furthermore, to have insights on the government's perspective on the EU interoperability framework and how it might affect the private sector. The interviewee is an IT architect in the development of MitID. Therefore, having knowledge on the subject and contributing with valuable insights on the development process.

Calcabis

Calcabis provides a platform with the aim to "integrate and work with all data sources, data sets and any human expert knowledge you possess" (Calcabis, 2018). The platform automates manual processes by using artificial intelligence (AI). Calcabis's primary industry is FinTech and RegTech. They help organisations become more efficient and assist them in dealing with regulatory requirements through compliance. Currently the company consists of a team of 16, including developers and business development members (Rost, 2018). The company was chosen because of their experience in automation such as integrating different data points and technological knowledge in general. Their capabilities and knowledge on combining technology and regulations was an inevitable fit with the research topic of this paper. Additionally, the interviewee is the CEO and provided knowledge and ideas on how data attributes could be integrated into one e-ID solution.

CMP Company

CMP Company is a creative full stack development firm established in 2016. The aim of the company is to create cutting edge technological solutions for its customers (CMP Company, 2018). Their primary industry is technology design within MedTech, FinTech and B2C start-ups in general. Currently, the team consists of 11 employees, including developers and designers (Christensen, 2018). The company was chosen because of their vast experience working with different start-ups and their capabilities of understanding the diverse needs of start-ups including regulatory compliance and concept proofing. The interviewee is the CPO, and is interested in looking for patterns in technology and has previously worked in a large corporation.

CoinstIntel

CoinsIntel is a project in early development. The project started in early 2018, with the aim of developing a cryptocurrency platform. The platform displays an overview of cryptocurrencies available, as well as, their market value and price. Additionally, it provides news, events and historical price graph on cryptocurrencies (CoinsIntel, 2018). Currently, their primary industry is FinTech and the team consists of two. The interviewee is a co-founder of the project. Though the project has not been established as a company yet, the interviewee has knowledge on identity management and technology such as the Blockchain. The actor was chosen because of his knowledge on the subject, as well as, his ideas on the future of identity (Mikula, 2018).

MEDEI Aps

MEDEI is a health IT company established in 2013. The aim of the company is to "improve health through the combination of medical expertise and engineering" (Bergsteinsson, 2018). The company provides a platform called "SMART-TRIAL" that assists medical device manufacturers in reducing the chaos that surrounds data collection and management in clinical trials. Their main industry is MedTech and currently the team consists of 16 employees, full-time and part-time (Bergsteinsson, 2018). The company was chosen for the role identification plays in the health sector and MEDEI has relevant input as a private actor. Additionally, the interviewee is the VP of Global Business development and has a background in biomedical engineering.

The following table shows an overview of the actors chosen within the private sector, including size, industry and product or service. The actors were chosen because of their relevance to the topic, start-ups working within innovative industries. The Agency of Digitisation is not included in the table as the actor represents the public industry and because of the research focus of the paper, is not included in the table.

Table VI: Background information on actors chosen.

Actor	Size (nr. of employees)	Industry	Product/service
Calcabis	16	RegTech/Fintech	AI platform
CoinsIntel	2	FinTech	Cryptocurrency platform
CMP Company	13	MedTech/Fintech/other B2C startups	Tech solutions
MEDEI	16	MedTech	Clinical trial platform

It is important to mention, despite the fact that The Agency of Digitisation is not mentioned in the table the knowledge provided in the interview was used in showing the status quo of e-ID in Denmark today. Additionally, it contributes with a perspective from the public sector which adds value to the results of this paper.

4.6. RELIABILITY

The aim of the study is to "reflect reality at the time they were collected, in a situation which may be subject to change" (Saunders at al., 2012). For that reason, replicating the research might provide different findings on the topic. First, errors such as participants bias may affect the findings, as the questions were tailored to the theory of interoperability before conducting the research. Second, because of the volatile nature of the topic, findings could change if the study is replicated in the coming years as technology continues to grow at a quick pace. Third, as the aim of this research is to show a snapshot in time, from the perspective of start-ups, replicating the study might undermine the research goal. However, the method section provides a detailed description of the research design, approach and interview guide (see appendix A) the process is reliable as it is replicable.

4.7. VALIDITY

A high level of validity was achieved by doing semi-structured interviews where participants were provided with sufficient time to explain their ideas and share their opinions. A mix of clarifying and probing questions were asked to allow the exploration of responses and themes from a variety of angles (Saunders et al., 2012). The interviews collectively resulted in six hours of qualitative data gathered. Additionally, the findings showed a relationship between interoperability and innovation as well as answering the research question. Based on this the validity of the research can be considered as high.

4.8. GENERALISABILITY

The aim of this research is not to provide generalizability for factors that foster innovation. The factors might vary when applied to different fields. For the purpose of this paper the factors identified are tailored to the field of e-ID at the time the research was conducted. The results in this study are not generalizable, although the research could be replicated in other fields. However, due to the newness of the topic the results are a snapshot in time and the factors that lead to innovation can and will change due to the volatile nature of technology. However, it would be interesting to test the generalizability of the findings and conclusions on the factors that foster innovation in other industries and to test if interoperability leads to innovation.

5. ANALYSIS

This section of the paper analysed the data collected through interviews. The data was analysed to discover how interoperability can foster innovation in start-ups when applied to e-ID systems. To answer the research question, the data collected was compared against the interoperability framework that comprised of four different layers: data, technology, human and institution. By analysing the data against the framework, the relationship between the layers was found. Furthermore, how those layers together could drive innovation. We state the theoretical findings based on which we could state the practical findings. On identifying the relationship between these interoperability layers and innovation we further sought to prove how interoperability could foster innovation. To do that we further identified factors that foster innovation when tailored to the context of e-ID.

5.1. PROBLEM FINDING

The first round of interviews can be classified as problem finding. The first interview conducted was with an actor from the public sector. It helped in navigating through the existing solution NemID. Additionally, it contributed to the understanding and development of the existing problem area and helped in creating the research question. Following that the interviews conducted were with actors from the private sector. The first round of interviews showed that current national e-ID systems are not efficient enough because of the lack of interoperability between countries. This lack of interoperability is due to the technological infrastructure on which these systems are built. Most systems are built on legacy systems and the requirements that these e-ID systems fulfil have advanced with the change in times. Public and private actors agreed that the existing solution is missing more verification attributes to be effective. From the start-up perspective, operating in an international market, the current national e-ID system does not serve their purpose because of restriction to one market, in this case, the Danish market.

Private businesses use the current e-ID only for administrative purposes, to keep track of financial expenses within the company or for checking on employee expenses. They believe the steps in using the national e-ID are more complex than creating their own verification process, such as a receiving an access link via email, login or a two-factor authentication. The benefits of using the current national e-ID system are low. All actors agreed on the need for an interoperable e-ID system that takes innovation into consideration. The actors could see potential in using a national e-ID system, one, if it had more attributes (verification points), two, no single market restriction, and three an innovative solution. More, a solution that is easy to use, transparent, built on modern IT infrastructure and serves an international market. Until now the existing e-ID systems have fulfilled the needs of businesses, but, with continuous advancements in technology and the need for businesses to continue to offer competitive products, an innovative e-ID system is needed.

5.2. INTEROPERABILITY

As mentioned the occurrence of interoperability can be evident through the four layers: data, technology, institutional and human (Palfrey & Gasser, 2012). The layers are interconnected and therefore the analysis of the technology and data layers were combined. The same goes for the human and institutional layers.

5.2.1. TECHNOLOGY & DATA

Technology and data are interconnected layers and foundational in creating interoperability. First, to achieve interoperability the data has to be readable and understandable across systems. Second, the technology used in exchanging the data has to be efficient and effective for the transaction to occur (Palfrey & Gasser, 2012). All actors stated, data as being valuable for companies today, more precisely the access to this data and the ability to analyse that data.

"Data is gold nowadays. It's not the system supporting the data. That's valuable as well but it's the amount and the quality of the data and how to use it against each other" (Rost, 2018)

According to three of four actors interviewed, the most important factor in achieving data flow across systems is the format of the data. Another finding that is aimed at maintaining data structure is the writing of the code for a product or service. Simple and clean code can enable systematic efficiencies which means it can be easily shared across systems. The cleaner the code the more efficient the system. This could lead to a more sustainable way of coding because of its applicability in reuse and integration with other code. In relation to data format, two actors mentioned that the data has to be understandable by both systems. Businesses collaborating with different structured data might have complications in accessing information systems or databases. A common data format between systems can be accepted by both system participants. However, a communication plan could be a solution to the problem where expectations about format and responsibilities are outlined.

"[The golden standard today] ...structure or format or communication structure. How do we deliver data to you, how do we get data from you? Those kinds of issues" (Bergsteinsson, 2018)

With the ability of data to flow across systems in a structured way it raises the issue of privacy and the access to sensitive data. Therefore, a system has to allow access to information and at the same time have strong security measures related to who is allowed to access the information. API is one solution to access systems as it allows data flow regardless of the quality of the systems.

"So, I can have a completely shitty system and you can have a perfect system that doesn't, you know, speak together but we can still make the flow of information set up and communicating to each other by having this little interpretation." (Christensen, 2018)

Although the actors all agreed on the benefits of using an API, they also addressed some concerns. First, the business accessing the system through the API, has to be validated beforehand, especially when handling sensitive information such as identity data. Second, the API has to be of high quality, particularly in sectors such as healthcare and finance where the volume of sensitive data is high. Furthermore, in relation to accessing data, a software development kit (SDK) was one of the solutions mentioned. The technology is similar to API; however, it is not active but stored on a local service. The benefit in using SDK is the offline connection, potentially useful in countries where there is lack of access to the Internet at all times. Three actors mentioned the importance of biometric technology such as face recognition, fingerprint and eye recognition. As digital attributes can be compromised, physical attributes are essential, especially in verification and authentication.

"Whether it's a fingerprint or a retina scan or something totally different. But it has to be somehow related to the physical us." (Bergsteinsson, 2018)

Furthermore, actors were asked their opinion on technologies such as Blockchain and cloud computing in regard to flow of information across systems. Interestingly, the findings suggested the benefit of Blockchain in the healthcare sector which would provide transparency. This is visible when accessing patient history and the ability to track patient consent history. An additional finding, is the possibility of several highly trusted entities creating a consortium. It could be built on Blockchain where information would flow and the entities would be monitored. This would help the issue of access and control as businesses would feel some level of trust due to the traceability and transparency. As for the cloud, one interviewee recommended the technology being on premise, as in stored locally because of the centralized structure of the technology. However, while another mentioned the cloud being the most secure infrastructure in the world. The most important finding from the research was related to validation. The nature of the Blockchain and the cloud differs as the Blockchain is decentralized and the cloud centralized. In both cases, the it raises the concern about authorities of the technology, as in who monitors the information flow.

> *"So, advantages and disadvantages to move to the centralized. For people, it's better to be decentralized, for companies, private sector maybe only for private sector, to go to decentralized for them it's a problem. Because they are using control and power and so on."* (Mikula, 2018)

AI technology was addressed in the case of connecting attributes or verification points to the previous mentioned technologies. AI technology such as machine learning will be used in the coming years because of increased usage of social networks, for instance Facebook. Additionally, implementing machine learning on top of the mentioned technology could have the potential of not only connecting attributes but also identifying risk factors. Furthermore, for the technology and data layers to be effective the human and institutional layers need to be introduced. To leverage the full potential of the technology and data layers there warrants action on part of the human and institutional layers.

5.2.2. HUMAN & INSTITUTION

As explained in the theoretical framework "the human and institutional levels of interop tend to build on top of technology and data layers." (Palfrey & Gasser, 2012). However, for the data and technology layers to leverage businesses cooperation and warrant action the human and institutional layers become vital. When two separate businesses cooperate, there is a need for alignment of work processes and mutual understanding between the individuals working together. The data and technology layers maybe setup to work efficiently however, certain situations may warrant an action on the part of the individual. For example, an internet of things (IoT) system collecting patient data can be set up efficiently but if the patient does not select the 'ENTER' button the data will not be saved. This is a prime example that shows the need for the human and institutional layers of interoperability. This is further elaborated upon by the actors.

> *"But sometimes it is not as easy as just talking to another engineer sometimes you have to make sure that there actually are some users or people on the other end that need to do something to make the interconnection or the interoperability work."* (Bergsteinsson, 2018)

One of the findings from the interviews was the company culture. All actors mentioned that the company culture was a combination of a formal and informal set up. This also contributes to the communication procedures that the actors follow. The company culture can be reflected in the way employees conduct and complete their work processes. Based on company culture there arises certain standardized procedures of achieving task completion. As elaborated by an actor and correlated to the theoretical framework that connects the four layers.

> *"It's all about understanding complexity, yeah. So, building the right solution requires the right architecture and roadmap with partners. Understanding the foundation and goal of the product. And we resolve them with deep data analysis and system architecture planning, wireframes or design, use case reviews and lots of tests."* (Christensen, 2018)

Start-ups and companies alike, that function on the international market need to account for the individuals that they are communicating and working with and the inherent differences in understanding technology and terminology. Therefore, there needs to be a combination of the institutional layer where the communication guidelines are laid down and the human layer where the language is common. Furthermore, these companies have to account for the cultural differences between individuals that can cause conflict if not attended to.

> *"So, the best way of ensuring that they understand what we are doing and how they should do it is to deliver to them some kind of documentation to understand this is the way we communicate this is how we handle security. So, they won't have to question how to do things or if it is secure enough in how you communicate"* (Bergsteinsson, 2018)

Furthermore, emphasized by the actors was the need for managing expectations and accounting for risk. As with all technology, there is risk involved. To test the efficiency of the system the human layer needs to act on the technology layer. Also, there is a chance the human might make an error however, experienced companies can warn future users and customers of past human error to avoid it in the future. For this to happen there needs to be communication between the involved entities.

> *"Like do not put your credit card information into this field because it is visible to everybody and they will still do it. And it is difficult and that is the most difficult part to new technology in general. If you cannot by any means eliminate such an error using your software or hardware you will risk people making an error. So, if a mistake can happen it will happen. So that is the most difficult part and the biggest challenge developing technologies"* (Bergsteinsson, 2018)

The findings state the challenges that businesses face when working with users and businesses. The problem, when viewed through the lens of interoperability, points toward the human and institutional layers together. At the institutional layer the businesses have to ensure that the involved teams work together in the most optimal way. At the human layer individuals have to work together through effective communication. For the involved businesses to cooperate there needs to be an agreement or alignment of the business process to achieve the shared goal.

"The challenges when we working with somebody that has some kind of a service or device that needs to connect or communicate with us the biggest challenge is probably to get them to understand first of all how it works and to ensure that they understand that we fulfil their security requirements and our security requirements at some level" (Bergsteinsson, 2018)

Based on the findings it is evident that all four layers have to be present to achieve a high level of interoperability. It further shows that these layers are interwoven. For the technology layer to work, individuals in the human layer have work together. Additionally, for the data layer to work it needs to be supported by the technology layer. Thus, proving that to achieve a high level of interoperability the layers have to align.

"Yeah, usually it is a link right of several people so it is not just someone being really good at developing something it is also the thoughts and the process behind it that I think has formed a lot of these concepts with AI and I think these things are also creepy but also wow" (Christensen, 2018)

The following table displays the findings that each actor stated relating to the interoperability layers.

Table VII: Quotes from actors on the four interoperability layers.

Actor	Data	Technology	Human	Institution
CMP	Basically, it all comes down to when are we talking 01101 you know kind of language. Because then it is not an interpreted language like PHP or CSharp. All these our languages that some people look at all times developers thinking that you know we have to make	So what the banks are really screaming for is a system that could possibly go in and help them in the way of saying that any information sent from your bank, you know it's us. Because we can integrate that into forms today. It's not a problem but it's not easy. That means that any mail or SMS or phone call you get for foreign companies you	Yeah, usually it is a link right of several people so it is not just someone being really good at developing something it is also the thoughts and the process behind it.	You want standardized ways of basically protecting yourself. So, you don't get people in that ruin your company

	this much easier for someone to understand if we want to build upon that.	can flag them. You can start using AI, machine learning, so the moment I get one report it's stopped.		
MEDEI	Everything that you would call data or information in our solution is stored either encrypted in JSON format using NOSQL or in clear text in JSON format using NOSQL. So, everything that is personal or identifiable is encrypted everything that is not which is operational data or time stamps other functional data that we need to support the usage of our service is not encrypted.	Okay so the technology which we use is open source yes. So our technology is built on a web application framework that's called Angular JS from google and another framework JavaScript framework for database communication and API that's called NODEJS and ExpressJS and all of these are open source so it is free to use but we of course have to develop code program how we want them to work and cooperate and all of these put together and you code what you want to do and what you want to be able to accomplish you get an application that is basically what it is.	And that is probably one of the biggest challenges. It is for example asking users to remember all sorts of things like press button number 2 to make sure that the data you need to communicate between the two is actually sent.	The only way to ensure that we do not run into problems with that kind of an issue is to take it up with our partner beforehand and discuss that we have actually experienced this before and even give guidance on that.
CoinsInt.	But for instance, if this information such as your medical information or something where the data is highly sensitive and cannot be exposed to third party then I think the Blockchain could be a very nice solution.	So, the technologies are basically JavaScript and JS is called.		
Calcabis	The more data points the better. Yeah but again the more data points the better. Data is gold nowadays. It's	Of course, we have the basic stuff as Java, C++ and other types of programming languages. If you are referring to		

	not the system supporting the data. That's valuable as well but it's the amount and the quality of the data and how to use it against each other.	Blockchain then no. It is basic technology and AI.		

From the data collected, only two out of the four actors referred to all four of the interoperability layers. The table depicts the important quotes that match the interoperability layers. Based on the findings and as stated in the theoretical framework there is a need for all these four layers to be present to achieve interoperability. When applied to the context of e-ID these layers are needed to develop and create a solution that is interoperable and open to innovation. The adaptability and flexibility of the solution can be seen through the layers which also contributes to the adoption of such solutions. Based on these findings we developed an e-ID solution that was created with the interoperability layers in mind.

5.3. GETTING TO AN INTEROPERABLE E-ID

As aforementioned, based on the findings it became evident that companies are only using the existing e-ID solution (NemID) for administrative purposes. As displayed below, a problem was identified. First, the existing e-ID solution was not efficient and second, it was not useful for the companies as they operate on an international market. As such, the existing solution is only applicable to the local national market which was its intended purpose at the time of creation. When the interviewees were asked the question: *What do you use NemID for?* they all stated the limited use of the national e-ID.

> "*Administrational/financial related work". "Because the infrastructure they use for their technology was already outdated when they launched it, which means that, few years ago when we first started to use NemID for a company for example we had to use a specific browser to be able to login and activate it. They fixed that now but the process itself involved a lot smaller steps then I expected in order to get started with it originally. Especially if you are using the key card instead of a key generator. Which is what I use personally."*
>
> (Bergsteinsson, 2018)

"*We do not use it"*. "*The reason behind it is that we are not a service provider. The banks cannot come to us and we do not have a fixed solution for them. So, we are actually building on premise for them so we customize the artificial intelligence in terms of what they want us to build. So therefore, we are not in this data game. So, we do not use NemID."* (Rost, 2018)

"Well we have all the legal shit we have to do for whenever we meet a start-up. The NemID card that we have and what not. It's getting over the first like contract written and creating a form for the company and who does what, that's the boring part. And actually, it takes time. So, we use it there and from there it's not so much again. It's only every now and then when we need some transparency in the company.". (Christensen, 2018)

"*Well, if I use NemID, I'm pretty much restricted to only Danish people."* (Mikula, 2018)

Based on these initial findings NemID as an e-ID did not benefit companies in any way other than administrative and was just a means to an end. Therefore, these companies and companies alike need a more innovative solution that is applicable and relevant to modern standards. Because of the need for a novel e-ID system a practical interoperable solution was developed. It is based on the findings from the actors and the aforementioned problem. To build the most efficient e-ID solution the challenges within the private sector had to be identified. When the actors were asked the question: *What would you say are the top e-ID challenges for businesses in the private sector right now?* the challenges were related to technology and data.

"Technology. I don't think we have the right technology yet." (Bergsteinsson, 2018)

"I would say the technology part. Being able to work with new technology and embracing the new ways of thinking. For example, the government they know it is doable but they do not want to look into it because what is it and what can we gain and how much resources we need to spend. And also accessing correct and validated data." (Rost, 2018)

"*I would say the challenges the businesses phase often is the complexity of them". "I mean you can correct me if I'm wrong here, I did a little bit of research on this and it's basically when government tries to involve in tech and try to optimize so to say certain processes."* (Christensen, 2018)

"So, I guess that interoperability because different businesses using different authentication processes and also data management. So, the problem is how to connect those systems together. So, what I think, one way could be

Blockchain solution, which is basically not controlled by anyone but it can be verified on the Blockchain, the data, by anyone." (Mikula, 2018)

5.4. AN E-ID SYSTEM BUILT ON THE INTEROPERABILITY LAYERS

The theory, findings from interviews and previous identified challenges create a link to the practical solution. Based on the interoperability theory coupled with the findings a need for an interoperable e-ID solution became evident. Therefore, the following table was made in order to explain and match the layers to a potential e-ID system. Through the initial framework (see illustration I) introduced in the theoretical framework, the findings have been applied to the model to explain how an e-ID system should be developed with interoperability. Moreover, a prototype of an interoperable e-ID system will be introduced and further elaborated in the discussion section.

Table VIII: Linking the interoperability layers with a practical prototype.

Interoperability	An e-ID system developed with interoperability as its base can prove to lead to innovation. The findings suggest that an e-ID system needs to be flexible and adaptive to change. Additionally, the system needs to fulfil the verification needs of businesses and take into account an international user. The system needs to be built on secure technology and allow for diverse compatibility and be easy to use.
Data	From the findings the need for various data attributes was stated. For an e-ID system to fulfil its end goal of validating users the entire process of validation needs to be secure. Inclusion of multiple data points through cross referencing these points can increase accuracy in verifying identities. To address security these different data points come with different types of data e.g. location data, biometric data, social media data, unique ID number and picture ID data etc. However, for these data points to provide security and accuracy they need to work together and can be done so through technology. The technology needs to be able to allow for these different data formats to work together for the cross referencing to make sense as the data points become more accurate and secure when combined.

Technology	From the findings the e-ID system could be built on the Blockchain and stored in the cloud. If built on the Blockchain this would allow for decentralization and transparency. Each time there is an access request it can be traced and tracked. Additionally, identity attributes would be securely stored in the cloud. The e-ID system would be accessible through an API. It would allow two separate systems to integrate and share information. However, a concern from the findings was the quality of the API which needs to be secure to allow for data flow.
Human	From the findings the e-ID system can allow for trust between individuals working together. If users and employees receive a validation stamp then it is easier to trust that individual. The same goes for business partnerships. Through transparency and trust there can be more collaboration and communication between the involved entities. The human aspect can show the true efficiency of the system if it allows effective communication.
Institution	From the findings it was clear that the e-ID system would be an initiative from the private sector with support of the public sector. For the adoption of such a system the public sector needs to cooperate with the private sector. As per the theory there needs to be an alignment in goals so that they can work together and effectively communicate. This is not only in the development stage but also after implementation. Through the e-ID system both sectors can work together and share information to fight against fraud and support the digital single market. Through alignment they can use the system as an access gateway to the goods and services and in turn increase competition. However, the findings also state that achieving this kind of partnership might prove difficult.

From our above-mentioned findings the following key statements were identified.

(1) The actors do no use the existing solution (NemID) for purposes other than administrative.
(2) The actors stated the potential of using an e-ID solution if it fulfilled more requirements that international businesses face and to be built on technologically advanced infrastructure.
(3) The need for an e-ID solution to include various data attributes (verification points).

(4) The need for all interoperability layers, (data, technology, institutional and human) to be present for an e-ID system to be innovative.

(5) That possible current and future e-ID solutions need to verify those who authorize and control such solutions.

(6) The development of future e-ID solutions should be a collaboration of actors from the private and public sector.

(7) The possibilities and opportunities that e-ID can generate can result in some kind of innovation.

(8) The need for an e-ID solution that captures the digital attributes of a user that can verify it to match the physical attributes.

An improved interoperable e-ID system meeting these statements would lead to innovation through the factors found. The factors are described in the following section.

5.5. FACTORS FOSTERING INNOVATION WITHIN E-ID

The following factors were identified based on the interviews conducted. The analysis of the findings and the theoretical framework allowed for the identification of factors that can foster innovation. The factors are efficiency, trust and security, resources and collaboration. Furthermore, these factors lead to improved validation. The identified factors are a by-product of interoperability and foster innovation when tailored to e-ID within the private sector, more specifically start-ups.

5.5.1. EFFICIENCY

The first factor identified is efficiency. As interoperability leads to innovation when tailored to e-ID, efficiency of the system is a contributing factor that can encourage new products or services. Efficiency allows for the optimization of a certain process which can then allow innovation as a by-product. Customers and businesses can be validated through an e-ID system in a manner that is secure and based on intuitive technology that in turn results in efficiency. Companies can work together effectively through quicker validation processes. In the financial industry the ability to identify fraudsters and for authorities to take action can be optimized through an e-ID system. An example would be some situation where fraudulent individuals identify themselves as bank staff and mislead customers by asking for the customer's credit card information on a false pretence. By the time the customer realizes something is wrong and contacts the bank, the damage has already been done. Increased efficiency in validation process can potentially prevent such situations or at the very least speed up the repercussion processes. In this case, the bank can automate their manual processes, by using an e-ID system, and as a result the customer would know that what he or she receives from the bank has been validated.

5.5.2. TRUST & SECURITY

Trust and Security are important factors that an e-ID system can deliver. First, an e-ID system that is built on secure technology like the Blockchain or the cloud allows users and businesses to receive validation stamps from this e-ID system. Once a user or a business has been identified and authenticated through the e-ID system then they are validated which creates a level of trust. This has potential benefits for businesses as they can pre-screen businesses before creating partnerships. Accordingly, the partnership becomes more transparent from the beginning. Furthermore, the validation would take less time and lowers the risk in doing business with new clients. An example and an interesting finding of an e-ID system that facilitates security and trust is in relation to networks and protection of children. There is potential for an e-ID system to be linked with an app that uses location data on smartphones for parents to keep track of their children's location. This app notifies parents if their children are in danger zones as the safe zones are predetermined by parents. They can invite people into their network to protect children. In the big picture, the same system could validate individuals in society and create a community. Thus, creating an ecosystem where you can invite individuals into your network based on their track record.

5.5.3. RESOURCES

Resources proved to be a factor fostering innovation. As such, an efficient e-ID system reduces cost in resources. Employees spend a great amount of time on manual processes that would not be necessary with an improved e-ID system. Such as, within the financial industry, contacting clients in relation to uploading IDs into banking systems. Instead of doing that manually an e-ID system could be a solution where their identity once validated holds until it needs re-approval from the client. Additionally, less monetary resources will be spent in terms of identifying fraudsters, on boarding of clients and stolen passports or credit cards. Moreover, having an interoperable e-ID system would enable the private sector to use the system and will not have to spend time and resources creating login features.

5.5.4. COLLABORATION

Collaboration between different actors can lead to innovation through sharing knowledge and expertise. It leads to new approaches to doing things as a result of combining different systems and technologies. One of the actors mentioned the gaming industry as an example. In that case technologies such as augmented and virtual reality have impacted social innovation. Furthermore, a collaboration of different actors in an e-ID system can bring about a social change, because it is not only about creating technology, rather, making change and improving society. However, for innovation to happen the actors have to understand new technology and "embrace the new ways of thinking" (Rost, 2018). Another finding is the value of that phone companies can bring because of the amount of data they possess. A collaboration with the phone companies would provide innovative incentives where the data is used for validation purpose. Interestingly, the actors agreed that creating an efficient e-ID would be most beneficial with an initiative from the private sector. However, with the support of the government. To create an optimum level of innovation from the collaboration the government has to be ready to embrace new technology. According to interviewees, other entities are also needed to capitalize on innovation benefits, including technology companies such as Apple and Google and authorities such as the European Union and worldwide government organizations. Thus, collaboration can benefit companies by creating networks for shared collaboration.

5.5.5. VALIDATION

The above-mentioned factors were identified when interoperability was applied to field of e-ID. The factors are efficiency, trust & security, resources and collaboration. These factors become prominent through the interconnection of the different layers. The factors enable an e-ID system to result in innovation. The four factors mentioned above collectively contribute to an improved process of validation. Actors interviewed agreed that the current e-ID system is not efficient, in connection with innovation, because of lack of applicability to meet business needs from an international perspective. However, the actors put forth ideas on potential e-ID systems that are developed to account for innovation, which can be achieved through the inclusion of the interoperability layers. The benefit is that the customer does not have to go to through many steps in the authentication process using e-ID, however, the process could be much more efficient and effective in the future. For instance, having one login where the user only has to remember few credentials to login to every platform, both private and public. As such, using an e-ID system for the purpose of validating customers or users. From the findings, it became evident that an e-ID system could be used in the MedTech industry during clinical trials of medical devices where patients need to fill out forms.

An interoperable e-ID system would benefit in a way that the user is validated and businesses can be sure of reliability of the source that is filling out the forms. The benefits for the business would be (1) that they do not need an extra step to authenticate a user which is due to the efficiency of the e-ID system. (2) The transparency that the e-ID system would deliver would create trust for the individual filling out the form and for them to know exactly who is reviewing the data the submit. (3) This can lower the risk for businesses as they can track patient consent history and when and who filled out forms. (3) By using an e-ID system business do not have to spend resources on developing their own access management systems. (4) Additionally, the system would prove the validity to authorities where the users enter their own information instead of a business having to prove where the data came from. An improved validation through a more interoperable e-ID system will help companies that previously have been struggling in validating a business concept. This will allow business to create a new type of service that has not been possible before.

Following illustration shows an improved model where the factors identified are included.

Table VIII: Quotes from actors on the factors fostering innovation

Actor	Efficiency	Trust & Security	Resources	Collaboration	Validation (innovation)
CMP	Like I said I could see your product being actually used it would speed up not just our processes but I could go out and tell that whoever uses our systems are 100% secure in the content of if we see a bad guy it is not just having his trail but we actually know who he is	My company would use it in the process of actually validating. Let's say all your touching here is Security. Think of any concepts where you have kids involved, families. And e-ID for sure is important because it is all about inviting people into your network that you believe in.	And it's simple because banks have a manual process in how to do this. Because they have to investigate this. So they are actually looking for ways of actually when a bank communicates, how do they do it. And that could be a cloud service.	I think if I could actually convince the citizens so to say if I was allowed to actually get consent through this e-ID platform. I think you would see a lot more grass root projects. Because it is like a Kickstarter campaign. I would put up a concept and people would give me consent through this and I would know that this data is valid because it's through their own e-ID. I think that is interesting that	I would say that would be killer as a B2C concept right. To bring that in because the validation right that scares people away. Because I don't know, we have in most cases validate email or Facebook login right. That is pretty soft, the mobile number we could also do but you can get a mobile number for free anyways. So, there are ways to get soft validation but not the big one. And I think NemID

					could spawn some really crazy projects that would not have to go through all the boring processes because now it is just troublesome.	that would scare off anyone.
MEDEI	I think, for example, buying alcohol in stores could be greatly improved. By optimizing the ID verification somehow. Not just alcohol but any type of service that requires you to show how old you are. Or that you live in the correct country.	You can see how Apple is handling security and Microsoft as well with their cloud solutions. They are ten years ahead of any other governmental institutions, publicly related governmental institutions. But I mean just like Apple is doing with the biometric fingerprint answer securing all of the devices	So, with the cloud it is a chain of computers. And you can deliver information to people or services or technology that is continuous and always available and fairly cheap because you can lower the cost by having it accessible or provide it outside you own.	Apple, some of the other major processing companies, high tech companies like Intel or maybe Microsoft. The European union. They are the only governmental organization, worldwide government organization that has enough democratic support to maybe develop or innovate something that could be of a benefit for the whole world but only own population.	I mentioned for the private sector but having access something like a universal e-ID in general will definitely help companies that have been struggling before in validating a business concept that is not possible today to do it. That requires them to verify the person that is using their system or that will receive surveys in the system, or the solution or the product. So, it will allow people definitely to develop new type of services that have not been possible before.
CoinsInt.	They don’t have to create something by themselves. So, they can just use something that is already approved to work, it’s used everywhere and we don’t have to	But then again that account must be even more secure because there is only one point of actually failure or attack. So that’s where the Blockchain would come in and		It doesn’t have to be 100 percent like the Blockchain, it could be consortium. So that means that you have several highly trusted entities and they work together to maintain it. So	What could be improved in the future on the website is that authentication of users, so they can login and see for example their value of the portfolio of cryptocurrencies

	do pretty much anything else. We just reuse what is already created and proven to work. So that would be one benefit.	maintain this security.		there is no single entity in charge of the NemID but there are several.	and so on and one way how it can be done could be that so in the registration the user would create the username and password and that would be encrypted and hashed and that hash would be put on the Blockchain.
Calcabis	Yeah it will also give them a better ability to shift vendor. Shift to different bank or whatever. They can do it like that right? Usually when you need to change to a different bank you need to go through all these documents and all that. So, imagine if you could just say I want a different bank right now. Press start and they would have the information required.	If you need to do business with somebody it takes you one of a split second to paint the system and if he’s verified you could do business with him. So, it could be you know a step, an automated step before you try to do business with anybody. So, in that sense the risk would be of course lower without increasing the cost because you would just have an API and it would be done automatically.	Yes of course it will. I think that they would use less resources of being compliant in terms of you know looking into fraud, looking into on boarding, looking into stolen passports or credit cards. And I know it can reduce the cost and resources spent in a bank and law firms and auditors and all of those that need to have a picture ID. So, you could argue that resources spend and risk taking new clients would be less	I would probably go to the phone companies to see if they are willing to do some collaboration because they own a lot of data. Facebook is doing the same as they have such a vast amount of data but only on Facebook. Google can do it in a different way banks can do it in a third way. You need to find a partner that has the data that you need to have in order to validate that the person is who they say they are.	I know that banks are looking into NemID for verification, again it is not enough for them. This is only validating that the person is say who it says it is but that is only on a personal note. Then they have to look into all the different things that are important for a bank. Have you been on a PEP list have you been on a sanctions list have you been accused with fraud. It is all those things that is essential for the banks to know. Then they need to validate if that person is someone we want to work with. I can see he lives in panama and has companies across the globe is it a person we want to work with yes/no. That is the essential

					information that the banks need to have.

5.6. CONCERNS

An interoperable e-ID solution is promising; however, it has some implications including people losing their jobs, digital privacy, security and culture. As our analysis has shown, one of the benefits of the solution is that it will enable automation of manual processes. The problem is that at the same time there are positions within businesses that will no longer be needed which leads to employees losing their jobs. Consequently, there has to be some solution in retaining employees within the companies. Additionally, an interoperable solution leads to a large database of personal information. The data has to be securely stored and managed. Which leads to the concerns around power. As the solution could be used all over the world, there is a question around who is going to be responsible for keeping the data secure. However, it also depends on the nature of the technology. One of the findings from the interview is that it should be an initiative from the private sector, with the support of the government. Finally, market maturity and culture could impact the implementation of an interoperable solution. It is not certain that all cultures are accepting of the solution. Universal e-ID is hard to imagine in practice, a more realistic approach involves several versions of e-ID systems.

6. DISCUSSION

The objective of this research was to (1) determine if interoperability can lead to innovation when applied to an e-ID system, (2) identify how interoperability encourages innovation when applied to e-ID and (3) highlight the importance of an interoperable e-ID solution through a generic prototype. These objectives when fulfilled collectively can answer the research question of *How does interoperability foster innovation in Electronic Identification Systems?* The theory of interoperability by Gasser & Palfrey proved an effective starting point. The authors were chosen due to their holistic approach to interoperability to include data, technology, human and institutional layers.

From our findings the following key statements were identified (1) the actors do no use the existing solution (NemID) for purposes other than administrative. (2) The actors stated the potential of using an e-ID solution if it fulfilled more requirements that international businesses face. (3) The need for all interoperability layers, (data, technology, institutional and human) to be present for e-ID to be innovative. (4) The development of future e-ID solutions should be a collaboration of actors from the private and public sector. (5) The need for an e-ID solution to include various data attributes (verification points). The above-mentioned findings are highlights of the overall findings that lead to the contributions this paper makes. The next sections will explain the theoretical and practical contributions and their implications.

6.1. THEORETICAL IMPLICATIONS

The theory of interoperability is applied to the field of e-ID. This research contributes to the body of knowledge by first, identifying how the different layers collectively enable factors that foster innovation when applied to e-ID. Second, addressing the topic of e-ID from the perspective of the private sector.

Four factors are identified that foster innovation in an e-ID system. The factors are increased efficiency, increased trust and security, less resources spent and increased collaboration. These factors collectively foster innovation through an e-ID system as they lead to an improved validation of a user or a business. The factors identified can be connected to each layer of the interoperability theory. Interoperability within the human layer creates increased collaboration, interoperability within the institution layer results in savings in resources, interoperability in the data layer leads to system efficiency and finally interoperability within the technology layer leads to increased trust and security. The following illustration displays an improved initial framework which includes how the interoperability layers foster innovation in an e-ID system. When the framework is applied to e-ID, interoperability creates the four aforementioned factors, increased collaboration, less resources spent, increased trust and security and increased efficiency that foster innovation.

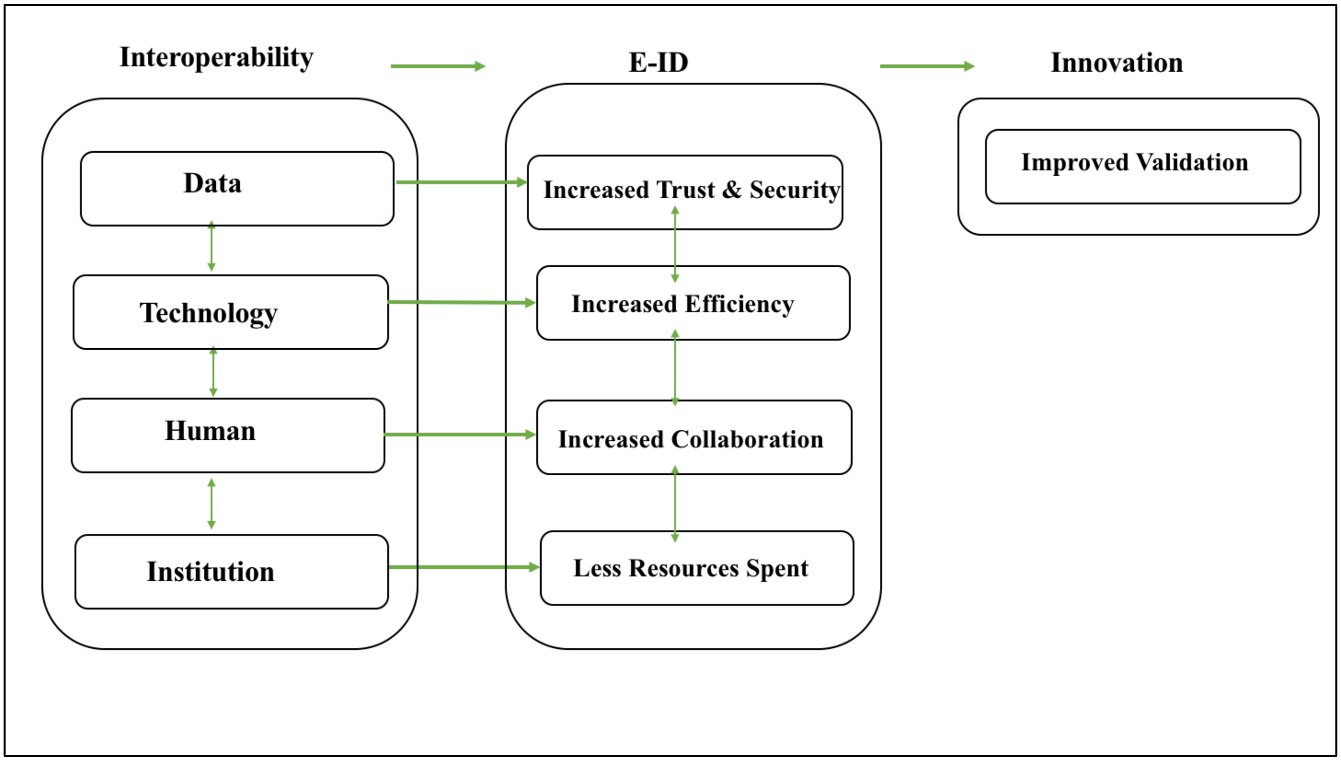


Illustration II: An improved initial framework.

As the interoperability layers are connected, so are the factors. They identified can be classified as the outcome of interoperability and the meaning of these factors change when applied to a certain context. The factors are a by-product of interoperability and have been found by other researchers. However, as mentioned the context is the differentiator. The framework has been applied to the context of e-ID, yet, it could be applicable to other industries. For instance, in electronic distribution systems, where interoperability has several benefits including efficiency "interoperability promotes a more efficient, reliable grid. It helps ensure both demand-side and supply side load management work cooperatively and productively" (ICF, 2016). Increased interoperability standards within tourism can lead to innovation through efficiency and cooperation. Further elaborated "cooperation among the agents in the tourism value chain with the aim to establish tourism services" as well as "sharing and reusing information among the agents in the tourism value chain to increase efficiency" (Baggio, 2014).

Even though the factors drive innovation their value can be potentially diminished. For instance, increased standardization can lead to system uniformity. This could hinder innovation leaving no room for adaptability and flexibility (Palfrey & Gasser, 2012). Additionally, increasing flow of information in e-ID raises the concern of data privacy, as in storing data in one database. Although the user sees a benefit in decreasing multiple logins, they might not feel comfortable in sharing large scale of personal information to businesses because of privacy concerns (Kinder, 2003; Six et al., 2005). Furthermore, this research contributes by including the human and institutional aspects of interoperability. Previous interoperability frameworks are focused on technological aspects, such as data flow in IS systems and business processes (AWG, 1998; IDEAS, 2003; Chen, 2006).

To address the management of e-ID systems we recommend a federated approach to be implemented. A federated approach should be followed to build interoperability, where actors involved do not have a common format rather share their resources. Creating an interoperable e-ID system following the federated approach allows the service to be more efficient and open for new technology (Chen, 2006). Furthermore, the system should be optimal for storing of the data, authenticating the identity owners, allowing the identity owners to define access rights for other users and evaluating access rights when answering queries (Koch et al., 2005). From primary and secondary sources there is a need to innovate through the inclusion of open standards to address scalability and the need to share expertise. One way of doing this is through 'Hackathons' where designers and developers work in teams to create prototypes for new products or services (Briscoe & Mulligan, 2014).

The findings show that the solution should be supported by the government. However, the actors have to be open for innovation. The actors should collaborate to reduce resources spent with the aim of creating something beneficial for all participants similar to aforementioned concept of hackathons, "users participating in the network design and build innovative products for their own use - and also freely reveal their design information to others." (von Hippel, 2007). The actors in the network are from various industries such as technology giants, regulators, universities and worldwide government organizations. These industries can create a solution with the support from the government, such as a federated innovation network, "heterogeneous pool of actors and tools that need to be identified and mobilized for effective cognitive and social translation across a set of diverse actors. The actors are organized into a hierarchically integrated control structure, mostly within a single firm." (Lyytinen et al., 2015).

An e-ID system should follow a federated approach, however, with the characteristics of a horizontal innovation network.

Though less resources spent can encourage innovation, it also leads to employees losing their positions. As manual processes become automated there is not much need for human resources. Consequently, there has to be a solution in retaining employees within the companies. Furthermore, as increased collaboration drives innovation there are obstacles that could diminish the value of the factor. Individuals understand technology differently depending on their personality and culture (Gasser & Palfrey, 2012).

6.2. PRACTICAL IMPLICATIONS

As aforementioned, this research seeks to contribute theoretically and practically. Practically, this research used the theoretical contribution as the base on which a practical solution was developed. The practical contribution is an e-ID solution that can help start-ups and businesses alike to further the mission of innovation but in a more secure and verified way. This eventually contributes to a safer and efficient digital ecosystem. Going back to the research problem, the main issue regarding interoperability and e-ID was the different national e-ID systems that are unable to work together (Arora, 2008). Through our findings this problem was due in large part to (1) The IT infrastructure (technology) on which these systems were built on which now are unsuitable and outdated. (2) The requirements and needs that these systems fulfil have changed due to the international scope that companies and products have (regulation).

These issues combined with the theoretical framework, the findings and the factors that foster innovation led to the development of an interoperable e-ID system. The identified actors that foster innovation sets out to answer the research question: *How does interoperability foster innovation through electronic identification (e-ID) systems?* With that in mind the developed solution accounts for the interoperability layers and the factors that foster innovation through an e-ID system. The practical solution enables companies on an international market to verify their users in a more efficient way. As the solution is not restricted to one market users can login onto platforms from all around the world and businesses do not have to manage multiple identification systems. For those requirements to be fulfilled the technology on which future e-ID systems are built have to match the modern standards. Therefore, the interoperable e-ID system is based on the model developed that includes the interoperability layers and adds the factors that foster innovation for an e-ID system. The image below depicts a prototype of the possible system which takes into consideration the findings and the aforementioned issues.

Following the image, the functionality of the system is explained, following which the forces that come into play when developing and maintaining such a system are discussed.

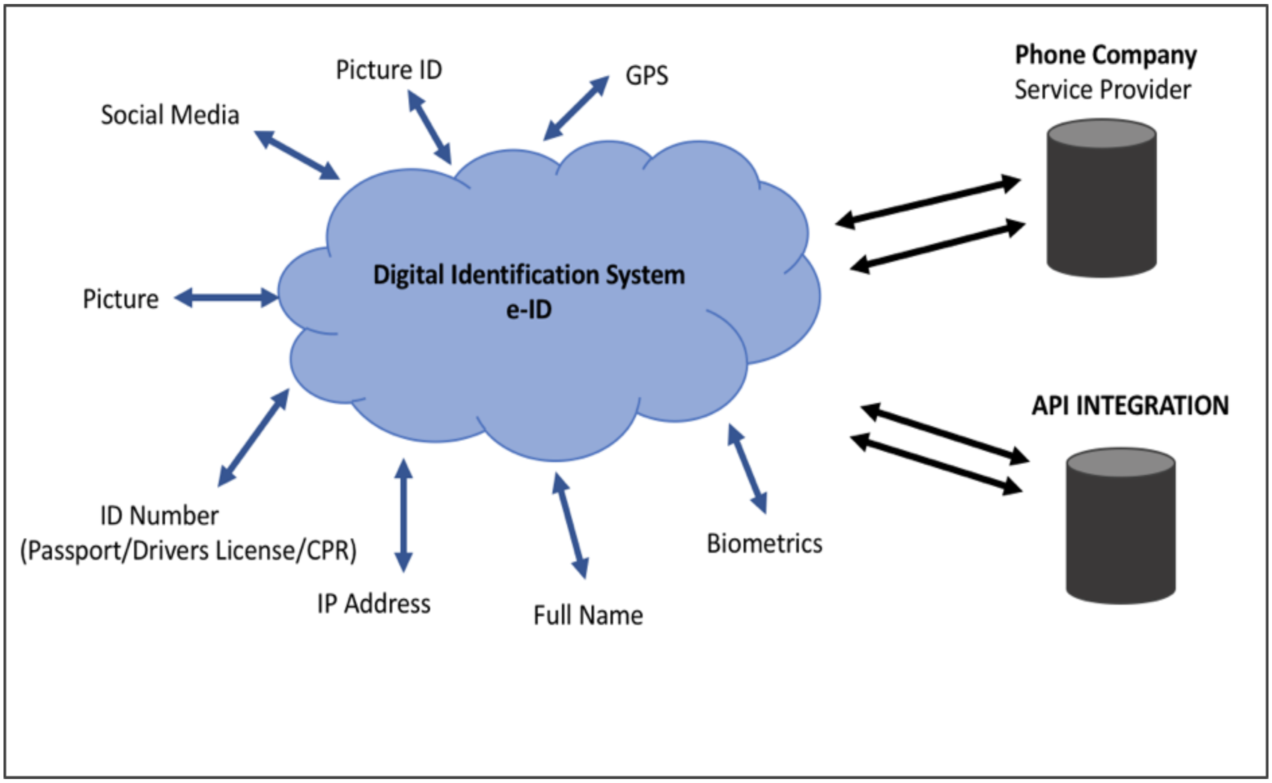


Illustration III: Interoperable e-ID solution.

The solution combines both attributes, having a login where users open an app by using their fingerprint or face recognition. The app then identifies the user by looking for attributes, such as full name, address, GPS location, picture ID, IP address, birth certificate and ID number (driver license, passport or CPR) and social media. Attributes such as social media, GPS or IP address can all identify an individual without a unique ID number. Furthermore, the information needed is provided by a service provider, which could for instance be a mobile network operator.

With reference to technology, the e-ID solution could be built as a "BlockCloud" or a cloud-based Blockchain. As such, several trusted entities around the world, public and private, creating a Blockchain consortium. By building a combination of Blockchain and a cloud, the power is not only restricted to one organization or country. This will also ensure the traceability of those who run the cloud which makes it more secure. Additionally, the solution is secure where the data is centralized in the cloud (storage purposes) but the traceability of the transaction is decentralized based on Blockchain (transparency purposes). To access the information there is an API solution. An API can be classified as having a high level of interoperability and openness because it is designed technologically on an open standard which can be used by companies to build upon (World Bank, 2018). The high level of interoperability that the API is designed to have allows it to be used as a mechanism for innovation by private firms.

The following explains the validation process the solution provides:

1. The service provider: To gain all the attributes that need to be validated and authenticated we require the main source of data. The optimal service provider would be a mobile network operator. Yet, the service provider is different in each country because of the nature of identification.

2. The cloud/Blockchain: The validation takes place within the cloud. The information stored in the cloud would be identity data provided by the service provider. This identity data refers to the verification points e.g. full name, GPS, IP address etc. These data verification points would be ranked based on the credibility it holds to validate the individual. The data points are ranked in a way that the most important one would be the most secure to identify that the individual is who they say they are. A limit or percentage of can also be set, if an individual match 80% of the criteria then the chances of the individual saying who they say they are is high.

3. API: The last step is an API integration that will enable businesses to use the software service by integrating it into their service. The BlockCloud would conduct the necessary checks and only then an individual or business can have access to the businesses platform or service.

The e-ID system presented above has benefits including efficiency, increased trust and security, less resources spent and increased collaboration. The main focus of this system is to put the verification in the hands of the network of verified entities. This in turn can create a trust circle between businesses creating a safe ecosystem. However, based on primary sources it is plausible to state that there will be a possibility that several different solutions will exist, such as one in the EU and other in the US. The two systems then have to operate on interoperable standards, to achieve optimal usage and to leverage the potential of the system. From the findings there is a need for electronic identification systems that are interoperable and modular. These systems need to be built on infrastructure that can capitalize on technological advancements. However, there are two facets that strongly impact these systems, technology and regulation. The solution presented above brings with it concerns regarding safety and security which will be discussed further.

6.2.1. TECHNOLOGY

The “BlockCloud” introduced has a positive and a negative side. The positive side of the Blockchain technology is that it promotes the idea of an ecosystem, creating a trusted network. Further described by Simons (2018), “in a decentralized system trust is based on attestations: claims that other entities endorse – which helps prove facets of one’s identity”. Developing an e-ID system on Blockchain technology is an argument for trust as businesses and individuals that access the Blockchain cannot undo the record. A new record needs to be introduced creating a ledger of transaction history. In this way it has a positive impact on both entities. Blockchain technology has proven beneficial, however, there is still scepticism around its use for electronic identification and access management. According to Olshansky and Wilson (2018) there is a need to further examine Blockchain and “an appreciation of the nuances in Blockchain security”. Iansiti and Lakhani (2017) refer to Blockchain as a foundational technology, “Blockchain is a foundational technology: It has the potential to create new foundations for our economic and social systems. But while the impact will be enormous, it will take decades for Blockchain to seep into our economic and social infrastructure”. Albeit the positive potential of Blockchain technology its adoption will take time as it is not a disruptive technology. However, the argument is still in favour of Blockchain technology as it will put the individual back in charge of his or her identity.

As the findings suggest, the different data attributes used to verify a user become more reliable when they are collectively used. The likelihood that an individual has a fake profile, passport, and driver’s license is relatively low. The cross-referencing of the data attributes can make the reliability of identification more accurate. This can be considered as a positive impact and used for risk mitigation (Trulioo, 2018). The more data attributes the better, this was reaffirmed from the findings and backed by secondary literature. There is consensus from both private and public actors on the matter. Future solutions need to be developed to fulfil requirements of different industries through the inclusion of multiple data attributes. Further elaborated, “it is in the smart cross-referencing of the right data through the right sources that the promises of new digital identity can fully take hold” (Trulioo, 2018).

Reflecting on the strengths of the data attributes some more than others. Biometric recognition uses an individual's unique identifiers like fingerprints, retinal scans, voice and facial characteristics to identify them. It has been around for a long time and can be considered as one of the more accurate attributes to identify and authenticate an individual. However, it has both positive and negative impacts on society. The positive impacts are the potential of inclusion for all including elderly, physically, and mentally challenged persons as it is easy to use as an attribute for identification (Thakkar, 2018). The negative impact is related to data breaches as biometric data is stored in a central database and if this data is accessible by a third entity then the data can be used for something other than the intended purpose. “According to calculations made by Sir Francis Galton (Darwin's cousin), the probability of finding two similar fingerprints is one in 64 billion even with identical twins (homozygotes)” (Gemalto, 2018d). This further enforces the accuracy of biometrics as an attribute for identification and authentication as it is interwoven with identity and should be treated as such. Therefore, even though it has positive and negative impacts the first outweighs the second. Furthermore, as argued for the need of interoperable systems as with new technology being developed existing solutions needs to be adaptable to capitalize on the developments. The future of biometrics will include user behaviour which is linked to service providers.

6.2.2. REGULATION

From the findings the actors suggested that governments developing e-ID systems need to incorporate the requirements of businesses and their potential international customers. Additionally, they stated that the public sector was slow in terms of capitalizing on innovative technologies and processes. However, contrary to findings the EU has introduced a new European Interoperability Framework that promotes seamless services and data flows for European Public Administrations (European Commission, 2018). The purpose of the framework is to guide public administrations to design and update their solutions to incorporate interoperability and to eventually contribute to the Digital Single Market. This is an example of how interoperability and e-ID can contribute to the digital economy and ecosystem.

Government authorities are looking to develop solutions with interoperability in mind. As evident from the European Union, their various efforts have resulted in the eIDAS regulation and the interoperability guidelines. The eIDAS “ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDAS are available” (European Commission, 2018). This is a step in the right direction. Furthermore, trust was a theme that repeatedly came up and rightfully so, “an EU-commissioned report published in 2013 found that fewer than one in four EU citizens "tend to trust" their national government and parliament. The number who trust the EU had also fallen from a high of 57% in 2007 to just 31%” (Gemalto, 2015). This further reinforces the need for interoperability of e-ID systems to facilitate security and safety. An e-ID system built on decentralized technology puts the user back in control which is needed. Although, sources show apprehension about government's ability to protect user data, the findings show a need for public-private partnerships (PPP). The World Bank Group, identify this type of partnership as a facilitator for developing e-ID solutions. These partnerships can allow for sharing of technical expertise. For these types of partnerships to be relatively successful there needs to be collaboration where both entities are open to sharing ideas to reach a common goal, e-ID. “Instead of thinking in traditional demand and supply terms, PPP actors need to focus on overcoming any legacy thinking and developing a shared thinking that comprises the mutual benefits of a common e-government infrastructure” (Medagalia et al, 2017). This reinforces the need for public-private partnerships which can eventually show trust on part of the government.

Although this section highlighted concerns about electronic identification systems there is a need to continuously develop digital solutions that can be scalable, dynamic and antonyms. The solution presented takes these ideas into consideration and only provides the first step. However, the main contribution is that e-ID systems require all interoperability layers to leverage the full potential and impact that it can have on the digital ecosystem. Conclusively, the future warrants for Blockchain technology to move from the theoretical to the practical as it will allow for decentralization and give identity control back to the owner. There will be more automation in identification and authentication processes with an increased focus on multi-factor authentication and single sign on which can be credited to interoperability. Lastly, regulations will enforce the need for access controls surrounding sensitive data that holds businesses accountable for breaches in security and usage of data without the consent of the owner (Sila, 2018).

6.3. LIMITATIONS

It is necessary to reflect upon the limitations faced during the research process and to state that this research is not without limitations. Most importantly, the research is conducted on the concept of e-ID which is in early development. Underlying factors such as technology and regulation are continuously evolving as the research is being conducted. The technologies mentioned in this paper such as distributed ledger technology, cloud computing and AI are relatively new in relation with e-ID. Furthermore, regulatory changes such as the GDPR and the eIDAS framework from the EU come to affect this year and their long-term effect is still to be determined. Therefore, the research shows a snapshot in time where results might be different in coming years.

Interviewing more actors within the firms could have given a better overview on their processes and tasks. However, this was not possible with the time restrictions and the lengthy nature that constitutes qualitative interviews. As the graph shows (see graph I), the researchers ended data collection when saturation was reached. However, as mentioned in the method section of this paper the graph is a paradox as with all research on reflection there are new ideas and ways that arise. The inclusion of additional interviews might cause the graph to look different.

Another limitation lies within the reliability and generalizability of the paper. Because of the novel nature of the topic, replicating the study might not give the same results. In achieving generalizability of the study researchers could interviewed more actors within the same company or added another method such as quantitative research to test the results. However, that was not the purpose of the paper and not feasible due to the limited timeframe. Finally, subjectivity of the researches has to be mentioned as a limitation. As such, the researchers of the paper interpret what is acceptable knowledge in relation to their understanding of society. However, others replicating the study may find that more or less interviews are needed depending on their chosen perspective.

6.4. FUTURE RESEARCH

This research presented interesting findings both theoretically and practically. However, the research only provided a first step in connecting the interoperability layers and innovation based on the cases chosen. There still needs further research and exploration into this connection. The findings presented form the base on which more theoretical research can be conducted to contribute to the field of interoperability and innovation. To further validate and generalize, future research can focus on including enterprises from varied industries. Additionally, SMEs that function on the local market rather than the international market. Future research can investigate the comparison between the business models of start-ups and enterprises to identify if interoperability and innovation have a direction correlation to the business model.

On completion of the methodological approach and when considering an alternative approach, a mixed method approach could have been chosen. The mixed method approach combines qualitative and quantitative methods. As such, the research could have begun with the quantitative method by creating and sending out a survey to enterprise companies. Once the data was obtained an overall understanding of the topic would be achieved and specific actors could have been chosen to conduct qualitative research with. Additionally, future research can use the factors that lead to innovation to research what kind of resulting innovation will arise when applied to the field of e-ID. Future research could focus on a single industry and a single company to uncover the need and benefits that interoperability brings with it.

As mentioned before, the example of a national e-ID is the Danish NemID. Currently, the ID is under transition and a new system will be introduced in the coming year. A replication of the study, after the transformation, is optimal. Additionally, since the eIDAS regulations comes into effect later this year the research can be tested by interviewing actors within the private sector after the implementation of the regulation. Finally, further research is recommended in other markets, including an international approach and choosing actors from

7. CONCLUSION

This thesis began with displaying the need for a safe and efficient digital ecosystem due to the high economic impacts of cybercrime. Through the research process it became evident that an electronic identification system can lay the foundation for the future. However, there are certain forces that affect the development of e-ID systems. These forces needed to accounted for when developing this type of system so that the full potential can be leveraged. Through the combination of technology, business, institutions and regulations an e-ID system can be developed to sustain the digital ecosystem. From the findings, the start-ups interviewed stated that existing e-ID solutions were inefficient due to (1) the IT infrastructure on which these systems were built on are now inadequate and outdated. (2) The requirements and needs that these systems fulfill have changed due to the international scope that companies and products have reached.

These problems become evident when viewed through the lens of interoperability. This can be observed with the diverse national e-IDs that exist and the lack of harmonization between them. Though previous literature points to technology and regulation as key forces that affect this harmonization, the institutions, businesses and citizens that use these services need to be accounted for. This research takes the view of the private sector, specifically start-ups in Denmark through semi-structured interviews. To uncover the underlying issues inbuilt in e-ID systems the theory of interoperability is the guiding lens that includes the layers of data, technology, human, and institution which allows for a holistic view. On using theory as a lens to collect data, the findings introduced the need for an e-ID solution that could include the interoperability layers.

Reflecting on the literature and adhering to the research question of *How does interoperability foster innovation through electronic identification system (e-ID)?* The answer can be found both theoretically and practically. The primary importance from the findings is the need for e-ID systems to be built with a level of interoperability that allows adaptability and flexibility in the future. This is reaffirmed and evident through the layers. At the data layer the formats and structures need to be in alignment for the flow of data across these systems which can be traced to the writing of the code. Simple and clean code can allow for reusability and programmability which can eventually allow for innovation. For the data to flow across the system the technology that enable this transfer needs to be secure. Therefore, technology like Blockchain and cloud were identified which can be accessed through an API. However, for the data and technology layers to prove effective the human and institutions involved need to be cooperate. The separate entities working together have to be able to communicate effectively through alignment of shared goals. Therefore, interoperability can lead to innovation when applied to e-ID systems.

However, to reach innovation all four layers need to work together to create an effective e-ID system. Therefore, theoretical and practical contributions were found. Theoretically, the contribution is the factors that foster innovation that are a by-product of interoperability that have different meanings based on the context. The identified factors are increased efficiency, increased trust & security, less resources spent and increased collaboration which eventually foster innovation. When tailored to e-ID the innovation can be classified as improved validation.

Practically, the contribution is an interoperable e-ID solution. A generic prototype is introduced. Because the prototype has not been tested the applicability cannot be stated however, it is a step in the right direction. The solution introduced can be built as a BlockCloud. Blockchain technology for decentralization, which allows for transparency and traceability of access transactions and requests. As well as, the cloud for data storage. The identification would be through an app that registers a fingerprint or face scan. The verification process would consist of multiple data attributes or verification points which would match the initial ID produced with the data attributes in the database. If the verification is positive then the individual is authenticated and eventually validated through the e-ID system. Businesses can access this validation system through an API to allow for integration of different systems. This type of system can benefit businesses in mitigating risks involved in new partnerships. The benefits can also be linked to customer relationship management and KYC checks. Businesses can also comply with regulations and corresponding legal liability by gaining user consent so they can continue to provide competitive products. The benefits for users can be for example, proving their identity online if their social media profiles have been hacked into. There are various use cases that support the need for electronic identification systems built on 21st century technology and standards.

Conclusively, an interoperable e-ID solution enables the identified factors to drive innovation. The result is improved validation for individuals and businesses. The topic of e-ID is continuously changing with advancements in technology and the introduction of new regulations. Therefore, there will be an increasing need for this topic to be researched from different perspective. However, electronic identification (e-ID) will continue to be a driver for digitally safe, secure and efficient economy and ecosystem. The readers of this paper may have not been victim to identity theft, hacks or other cyber related crime however, these problems are real and warrant action from those in power. Through this research the authors make the point that there is a growing need for inclusion of all humans in this digital economy. Furthermore, electronic identification systems will continue to be a viable solution in this era of data breaches. The readers of this paper may have not been victim to identity theft, hacks or other cyber related crime however, these problems are real and warrant action from those in power.

8. REFERENCE LIST

Agency of Digitisation. (2018). *About the Agency for Digitisation*. Retrieved from https://en.digst.dk/about-us/

Anthes, G. (2015). Estonia: A Model for e-Government. *Communication of the ACM, 58*(6), 18-20.

Architecture Working Group. (1998). *C4ISR Architecture Working Group. Department of Defence*. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a348567.pdf

Arora, S. (2008). National e-ID card schemes: A European overview. *Information Security Technical Report, 13*(2)*,* 46-53.

Avanzi, D., Foggiatto, A., Santos, V. A., Deschamps, F. & Loures, E. (2017). A framework for interoperability assessment in crisis management. *Journal of Industrial Information Integration, 5*, 26-38.

Baggio, R. (2014). Technological innovation in e-tourism: the role of interoperability and standards. *Tourism Management Marketing and Development: The importance of Networks and ICTs*, 41-55

Bergsteinsson, J. I. (2018). Personal interview.

Brinkmann S. (2014). Interview. In: Teo T. (eds) Encyclopedia of Critical Psychology. Springer, New York, NY

Briscoe, G. & Mulligan, C. (2014). Digital Innovation: The Hackathon Phenomenon. *Creativeworks London*. Retrieved from http://www.creativeworkslondon.org.uk/wp-content/uploads/2013/11/Digital-Innovation-The-Hackathon-Phenomenon1.pdf

Bryman, A. & Bell, E. (2007). *Business research methods (2nd ed.)*. Oxford, New York: Oxford University Press.

Calcabis. (2018). *We emulate people*. Retrieved from https://calcabis.com/

Chen, D. (2006). Framework for Enterprise Interoperability, in Workshop on Enterprise Modelling and Ontologies for Interoperability (EMOI-INTEROP)

Chen, D. Doumeingts, G. & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry 59*(7)*,* 647–659.

Christensen, D. (2018). Personal interview.

Clippinger, J. H. (2018). *Chapter 2 Why Self-Sovereignty Matters*. Retrieved from https://idcubed.org/chapter-2-self-sovereignty-matters/

CMP Company. (2018). *Collaboration makes perfect!* Retrieved from http://cmp-company.com/

Collis, J. & Hussey, R. (2013). *Business research: A practical guide for undergraduate and postgraduate students* (2nd edn.). Basingstoke: Palgrave Macmillan.

Daft, R. L. (1978). A Dual-Core Model of Organizational Innovation. *Academy of Management Journal*, *21*(2) 193-210.

Davis, G. (2018). *The Past, Present, and Future of Password Security*. Retrieved from https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/security-world-password-day/

Dillon, T., Wu, C. & Chang, E. (2010). Cloud Computing: Issues and Challenges. IEE International Conference on Advanced Information Networking and Applications (AINA).

E-estonia. (2018). *Estonia to receive Government Leadership Award*. Retrieved from https://e-estonia.com/estonia-to-receive-government-leadership-award-2018/

eIDAS. (2014). Directive 2014/910/EC of the European Parliament and of the Council of 23 July 2014

European Commission. (2015). *Conference on e-ID: A key to business growth and innovation*. Retrieved from https://ec.europa.eu/digital-single-market/en/blog/conference-eid-key-business-growth-and-innovation

European Commission. (2017). *E-Identification*. Retrieved from https://ec.europa.eu/digital-single-market/en/e-identification

European Commission. (2017). *New European Interoperability Framework*. Retrieved from https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

European Commission. (2018a). *Data protection.* Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en

FIDO Alliance. (2018). *About the FIDO Alliance.* Retrieved from https://fidoalliance.org/about/overview/

Gasser, U. & Palfrey, J. (2007a). Breaking Down Digital Barriers: When and How ICT Interoperability Drives Innovation. *SSRN Electronic Journal*. Retrieved from https://cyber.harvard.edu/publications/2007/Breaking_Down_Digital_Barriers

Gemalto. (2015). *Bringing eID to Europe: a question of privacy.* Retrieved from https://www.gemalto.com/review/Pages/bringing-eid-to-europe-a-question-of-privacy.aspx

Gemalto. (2018a). *5 reasons for Electronic National ID Cards*. Retrieved from https://www.gemalto.com/govt/identity/5-reasons-electronic-national-id-card

Gemalto. (2018b). *National ID cards: 2016-1018 facts and trends*. Retrieved from https://www.gemalto.com/govt/identity/2016-national-id-card-trends

Gemalto. (2018c). *Aadhaar: facts and trends 2017-2018*. Retrieved from https://www.gemalto.com/govt/customer-cases/aadhaar

Gemalto. (2018d). *Biometrics: authentication and identification.* Retrieved from https://www.gemalto.com/govt/inspired/biometrics

Greener, S. (2008). *Business Research Methods*. SBN 978-87-7681-421-2

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660.

Halperin, R. and Backhouse, J. (2008). A roadmap for research on identity in the information society. *Identity in the Information Society, 1*(1), 71-87.

Hammersley, B. (2017). *Concerned about Brexit? Why not become an e-resident of Estonia*. Retrieved from http://www.wired.co.uk/article/estonia-e-resident

Hoff, J.V. & Hoff, F.V. (2010). The Danish eID Case: Twenty years of Delay. *Identity in the Information Society, 3*(1), 155-174.

Iansiti, M & Lakhani, K. R. (2017). *The Truth About Blockchain.* Retrieved https://hbr.org/2017/01/the-truth-about-blockchain

ICF. (2016). Standards and Interoperability in Electric Distribution Systems. *US Department of Energy*. Retrieved from https://www.energy.gov/sites/prod/files/2017/01/f34/Standards%20and%20Interoperability%20in%20Electric%20Distribution%20Systems.pdf

ID2020. (2018). *Why an alliance?* Retrieved from https://id2020.org/partnership/

Kinder, T. (2003). Mrs Miller Moves House: The Interoperability of Local Public Services in Europe. *Journal of European Social Policy, 13*(2), 141-157.

Koch, M. and Kathrin Möslein, K. M. (2005). Identities Management for E-Commerce and Collaboration Applications. *International Journal of Electronic Commerce*, *9*(3), 11-29.

Kreps, G. L. & Neuhauser, L. (2010). New directions in eHealth communication: Opportunities and challenges. *Patient Education and Counselling, 78*(3)*,* 329-336.

Kubicek, H. (2010). Introduction: Conceptual Framework and Research Design for a Comparative Analysis of National e-ID Management Systems in selected European Countries. *Identity in the Informal Society, 3*(1), 5-26.

Linn, C. J. (2005). How terrorists exploit gaps in US anti-money laundering laws to secrete plunder. *Money Laund Control, 8*(3), 200-214.

Macknight, J. (2018). *Will the digital world solve the identity crisis?* Retrieved from http://www.thebanker.com/Transactions-Technology/Will-the-digital-world-solve-the-identity-crisis?ct=true

McAfee. (2018). *New Global Cybersecurity Report Reveals Cybercrime Takes Almost &600 Billion Toll on Global Economy*. Retrieved from https://www.mcafee.com/uk/about/newsroom/press-releases/press-release.aspx?news_id=20180221005206

Medaglia, R., Hedman., J. & Eaton, B. (2017). It takes Two to Tango: Power Dependence in the Governance of Public-Private e-Government Infrastructures. *Thirty eighth International Conference on Information Systems, Soul 2017.*

MEDEI. (2018). *About MEDEI - Technology driven innovation in healthcare*. Retrieved from https://www.medei.dk/about
Mikula, T. (2018). Personal interview.

Milanovic, N. (2017). *The next revolution will be reclaiming your digital identity*. Retrieved from https://techcrunch.com/2017/10/17/the-next-revolution-will-be-reclaiming-your-digital-identity/

Miller, P. (2002). *Interoperability. What Is It and Why Should I Want It? Ariadne Issue 24*. Retrieved from http://www.ariadne.ac.uk/issue24/interoperability?ref=SevSevil.Com

Modinis study. (2005). *Common Terminological Framework for Interoperable Electronic Identity Management.* Retrieved from https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc#4_13_Digital_Identity

National Geographic. (2018). *The Continuous History of the Passport*. Retrieved from: https://www.nationalgeographic.com/travel/features/a-history-of-the-passport/

NEHTA. (2005). *Towards an interoperability framework*. Retrieved from http://www.providersedge.com/ehdocs/ehr_articles/Towards_an_Interoperability_Framework.pdf

New World Encyclopedia. (2018). *Interoperability.* Retrieved from http://www.newworldencyclopedia.org/entry/Interoperability

Olshansky, S. & Wilson, S. (2018). *Blockchain and Digital Identity - A Good Fit?* Retrieved from https://www.internetsociety.org/blog/2018/03/blockchain-digital-identity-good-fit/

Palfrey, J. & Gasser, U. (2007b). Case Study: Digital Identity Interoperability and eInnovation. *SSRN Electronic Journal.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1070061

Palfrey, J. & Gasser, U. (2012). *Interop: The promise and perils of highly interconnected systems.* New York: Basic Books.

Porter, M. E. & Millar, V. E. (1985). How information give you competitive advantage. *Harvard Business Review*, *63*(4), 149-160.

Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs. *Identity in the Information Society, 3*(1), 175-194

Robson, C. (2002). *Real World Research (2nd edn.).* Oxford: Blackwell.

Rost, K. W. (2018). Personal interview.

Salyer, P. (2015). *The Road to Identity 3.0: From Microsoft Passport to the Internet of Things*. Retrieved from http://www.fourthsource.com/news/road-identity-3-0-microsoft-passport-internet-things-18707

Saunders, M., Lewis, P. & Thornhill, A. (2012). Research methods for business students (5th edn.). Pearson Education: England.

Schukai, R., Chadwick, S. & Baker, T. (2017). *Who are you? Defining digital identity and authentication technologies*. Retrieved from https://blogs.thomsonreuters.com/answerson/digital-identity-authentication-technologies/
Shen, J. (2016). *e-Estonia: The power of potential of digital identity*. Retrieved from https://blogs.thomsonreuters.com/answerson/e-estonia-power-potential-digital-identity/

Sila. (2018). *Trends & Predictions in Identity Management.* Retrieved from https://silasg.com/insights/2018-trends-predictions-identity-management

Simons, A. (2018). *Decentralized Digital Identities and Blockchain - The Future as We See it.* Retrieved from https://cloudblogs.microsoft.com/enterprisemobility/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/

Six, P., Raab, C. & Bellamy, C. (2005). Joined-up government and privacy in the UK part 1: managing tension between data protection and social policy. *Part I. Public Administration 83*(1), 111-113.

Swanson, E. B. (1994). Information Systems Innovation Among Organizations. *Management Science, 4*(9), 1069-1092.

Thakkar, D. (2018). *How Does Biometric Technology Impact Society?* Retrieved from https://www.bayometric.com/biometric-technology-impacts-society/

Trotman, R. (2017). *Identity Theft and Cybercrime Statistics.* Retrieved from https://www.globalcyberalliance.org/identity-theft-and-cybercrime-statistics.html

Trulioo. (2014). *The history of ID Verification*. Retrieved from https://www.trulioo.com/blog/infographic-the-history-of-id-verification/

Trulioo. (2018). *Data Attributes as the New Digital Identity.* Retrieved from https://www.trulioo.com/blog/data-attributes-identity/

UIDAI. (2018a). *About IDAI*. Retrieved from https://uidai.gov.in/about-uidai/about-uidai.html

UIDAI. (2018b). *Aadhaar Usage*. Retrieved from https://uidai.gov.in/your-aadhaar/about-aadhaar/aadhaar-usage.html

UIDAI. (2018c). *Features of Aadhaar*. Retrieved from https://uidai.gov.in/your-aadhaar/about-aadhaar/feature-of-aadhaar.html

Von Hippel, E. (2007). Horizontal innovation networks by and for users. *Industrial and Corporate Change, 17*(2), 293-315

World Bank Group. (2018). Technology Landscape for Digital Identification. *International Bank for Reconstruction and Development.* Retrieved from http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf

Yoo, Y., Henfridsson, O. and Lyytinen, K. (2010). The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research. *Information Systems Research*, *21*(4), 724-735.

Zmud, R. W. (1982). Diffusion of Modern Software Practices: Influence of Centralization and Formalization. *Management Science, 28*(12), 1421-1431.