TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Katariina Muru 153414IVGM

Global Trust Framework: Pilot for Smart Vaccination Certificates

Master's thesis

Supervisor:	Ingrid Pappel PhD
Co-Supervisor:	Eric Jackson
Co-Supervisor:	Richard Michael Dreyling III

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Katariina Muru 153414IVGM

Globaalne usaldusarhitektuur: Vaktsiinisertifikaatide piloot

Magistritöö

Supervisor:	Ingrid Pappel PhD
Co-Supervisor:	Eric Jackson
Co-Supervisor:	Richard Michael Dreyling III

Tallinn 2021

Author’s declaration of originality

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

Author: Katariina Muru

10.05.2021

Abstract

This thesis is written in English and is 57 pages long, including 5 chapters, 5 figures and 2 tables.

Annotatsioon

Globaalne usaldusarhitektuur: Vaktsiinisertifikaatide kaasus

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 57 leheküljel, 5 peatükki, 5 joonist, 2 tabelit.

List of abbreviations and terms

WHO	World Health Organization
EHR	Electronic Health Record
HIE	Health Information Exchange
HIS	Health Information System
WHA	World Health Assembly
EU	European Union
PHI	Personal Health Information
DT	Digital Transformation
API	Application Programming Interface
TAM/TAM2	Technology Acceptance Model
UTAUT	Unified Theory of Acceptance and Use of Technology
TRA	Theory of Reasoned Action
DOI	Diffusion of Innovation
SVC	Smart Vaccine Certificate
MoU	Memorandum of Understanding
KSI	Keyless Signature Infrastructure
HL7	Health Level Seven
DHIS2	District Health Information Software 2
PKD	Public Key Directory
PKI	Public Key Infrastructure
PHA	Public Health Authority

Table of contents

List of figures

List of tables

1 Introduction

The global pandemic caused by COVID-19 has changed the world as we know it. This means that there is a cross-sectoral demand to stop the spread of diseases that have such a high impact on our healthcare systems and economies. In order to restore global free movement, limit the potential spread of virus and also avoid vaccine-related frauds the guides on how to create national Smart Vaccine Certificates were created by World Health Organization and European Union. An important cornerstone for exchanging Smart Vaccine Certificates and health data securely is the Global Trust Framework that acts as a secure data exchange method. Global Trust Framework is built on the idea of universally accepted lists of trusted stakeholders in the health data ecosystem of each country [1].

As Estonia has a good reputation, competencies and knowledge of eGovernment on both local and state level [2], [3]then it is fair to state that they have a good starting position when it comes to The Smart Vaccine Certificates being the first practical use-case to pilot and test the Global Trust Framework. This is based on the same technology stack as Estonian X-Road. The piloting phase is important to create trust and prove the efficiency of this solution and to discover the legal, organizational and technical implementation barriers, opportunities and necessary amendments before fully deploying this solution to production. There are of course a lot of ethical concerns regarding vaccines, as there is a huge gap in the distribution of vaccines between countries, but this is not in the scope of current research.

The creation of digital standards is a process that usually takes years and is now forced into a short timeframe due to the ongoing global crisis. Just like the famous quote by Winston Churchill “Never let a good crisis go to waste“ says, this pandemic gives the WHO a unique momentum to transform itself and the eHealth domain in an effective and focused way. As WHO has accepted the role of serving as the global anchor of trust, then as a standards-creating body WHO must now undergo the process of digital transformation.

To understand the scope and importance of creating this significant piece of digital public good it is important to understand the current wider concept of eHealth, the opportunities and weaknesses it entails. The undergoing theoretical frameworks that are covered in this thesis are digital transformation, technology acceptance models, cross-border health data exchange, interoperability and of course trust itself. These are covered and analysed in the second chapter. In third chapter the Research Methodology is described, where the author of this thesis will give an overview of the chosen methodology, the data collection methods and the data sources. The fourth chapter gives an overview of the case, describes how health data is exchanged currently and describes the concept of global trust framework. The fifth chapter represents the research outcomes, discussion, conclusions, limitations and future developments of given case.

The first research question is "How is cross-border health data exchanged currently?" It seeks to describe the current cross-border health data exchange methods and their weaknesses. In order to achieve the aimed result following sub-questions will be addressed "What cross-border health data exchange methods/frameworks are in use?" and "What are the limitations of current health data exchange solutions?"

The second research question is "How can X-Road based Global Trust Framework be implemented for Smart Vaccine Certificates?" and for answering that the sub-question "What are the legal, administrative and technological barriers for implementing global trust framework?" is asked.

The author of this thesis had a wonderful opportunity to be a part of this international project team that is in the epicenter of the ongoing global crisis. Weekly meetings, knowledge-sharing workshops, semi-structured interview and project documentation gave a unique perspective of this phenomenon that students are probably going to research and discuss for years to come.

2 Theoretical Background

2.1 eGovernment

eGovernment is the use of information and communication technologies combined with organizational change to improve the structures and operations of government and help them deliver public services and transform relations with citizens, businesses and also other governments [4]. eGovernment covers the dimensions of public administration, democracy, governance and policy making [5]. Implementing eGovernment helps to change outmoded bureaucracies, improves the efficiency and effectiveness of public service and promotes participation and democracy [6]. In the core of eGovernment is public management modernisation and reform, that uses technology as a strategic tool to improve structures, processes and legal framework in order to increase public value [5]. In the current thesis the research focus is on one specific domain of eGovernment - the healthcare domain called eHealth.

2.2 eHealth

eHealth is defined by the World Health Organization (WHO) as the "use of information and communication technologies" for health and this is one of the most rapidly growing areas in the health domain today [7]. eHealth can also be described as an umbrella concept that covers different terms from telemedicine, mHealth to tele-care and tele-health [8] but it still refers mainly to combining conventional forms of prevention, care and diagnostic with digital technologies. Implementing eHealth systems has enhanced the accessibility, responsiveness and affordability of health services and also improved health services both locally and internationally [9].

Physicians have traditionally and historically given the Hippocratic oath that includes the phrase "First do no harm" (latin. *primum non nocere*), but medical errors still happen due to missing information and unknown patient health history. In order to decrease medical errors the healthcare domain has been standardizing and optimizing the electronic distribution of accurate information to the physicians [10]. This leads us to the next important term - Electronic Health Record (EHR) - that is considered to be the core component of eHealth. EHR is described as "digitally stored health related information about an individual's lifetime, with a purpose to support shared care, education and research" [10]. EHR is considered as a tool that (if fully implemented) could have many benefits due to enabling the access to important information that improves the efficiency of physicians, becomes a basis of patients complete lifelong records of medical interventions, reduces costs compared to paper-based health records, improves the communication between different systems, organizations, countries and last but not least provides statistical data for analysis and research [10]. There are of course many challenges, such as lack of standards that leads to different implementations of EHRs and legal, security or privacy issues. Due to these challenges concerns about the reliability and generalizability of using EHRs rise and that is a problem that this sector is facing.

Health Information Exchange (HIE) concept was recognized already in 1957 with the rise in occupational health problems in the United States when the need for a central coordinating organisation arose [11]. Since that the description of HIE varied widely until after analysing different versions a definition was proposed as "the electronic mobilisation of clinical and administrative information within or across organisation in a region or community and, potentially, internationally between various systems according to locally and/or nationally recognised standards while maintaining the authenticity and accuracy of the information being exchanged, enabling stakeholders to make informed decisions to enhance healthcare quality of a patient and population" [11].

Health Information System (HIS) is a term that Peter Reichertz introduced already in 1984 [12]. HIS is described as "a system that captures, stores, manages or transmits health information of individuals or the activities of organizations that work within the health sector" [12]. It's main objective is to improve the slow and inefficient services in hospitals by moving from paper-based to computer-based processing and storage of health data [12].

2.3 eHealth History

WHO was created in 1948 and it is a science based international organization of 194 Member States with its primary role to direct and coordinate international health. WHO is a standards producing body that gets its mandate from the World Health Assembly

(WHA) that is the decision-making-body of this WHO. WHA is an annual event that is attended by delegations from all the Member States and it determines the policies of WHO [13]. The first time WHO recognized the increasing importance of the Internet and its potential to impact health was already in 1998 [7]. The first eHealth strategy was then established in 2005, as the WHO urged all the Member States to draw up long-term strategic eHealth development and implementation plans [14]. Since then eHealth related resolutions and deliberations have been mentioned in 2013, with the focus on health data standardization and in 2016 and 2018 on the importance of mHealth in health service delivery and public health [7]. In 2005, WHO also launched the Global Observatory for eHealth with its mission to improve health by sharing information and guidance on best eHealth practices and standards to Member States [7].

Since the 1960s, eHealth in Europe has also grown from research and development initiatives to governmental and global strategic objectives in most countries. And while the European Union (EU) Member States are individually responsible for providing healthcare, the problems and challenges that national health systems face are problems that the whole EU faces [15]. The interest and need to digitalise the healthcare ecosystem is a EU strategic objective, activity and policy. Directive 2011/24/EU states that all the EU Member States must provide "safe, high quality, efficient and quantitatively adequate healthcare" to European citizens on their territory [16]. In order to be able to provide healthcare on this level, the exchange of health data under the principles of Data Protection Act is necessary and therefore as a further step in this Directive the Article 14 promises to create a eHealth network that connects Member States' national authorities. The cross-border health data flow is not only vital for medical care, but it also enables to improve public health and supports research. So the main objective of eHealth network is to deliver interoperable applications that ensure access to cross-border healthcare [16].

2.4 Opportunities and Challenges of eHealth

As the world ages and our population gets older the healthcare costs grow also due to dramatic increase in diseases that are caused by unhealthy lifestyles, expensive new technologies and higher need for health and social care. According to Toomas-Hendrik Ilves, the largest problem we face is eHealth "lagging at least 10 years behind virtually every other area in the implementation of IT solutions" [17]. There are also legal, ethical and governance issues. The biggest problem with law is that on one hand it defines the norms and context, but most of the time is behind from systemic and organizational changes as it takes too long to get established and applied [18]. Therefore it is essential to focus on developing and redefining our eHealth model to ensure that the healthcare services are delivered efficiently and with quality to those who are in need.

In 2004, the European Commission started to work towards legal clarity of eHealth products and services. Since this day there is no single piece of legislation that covers eHealth and brings legal understanding. Rather there are a lot of national and Europe-wide sets of legislations, which makes navigating in the legal sphere of eHealth quite difficult. The biggest ethical concerns are related to the growing amount of information and its integrity and authority. On a governance level the complexity of eHealth is mostly related to finding a common standpoint between eHealth and its service to health systems and services [18].

eHealth main beneficiaries are citizens, patients, healthcare professionals and also health related organizations and public authorities [17]. Proper implementation of eHealth makes healthcare more personalised, targeted, effective, helps to reduce errors and the length of hospitalisation and lastly increases the patient satisfaction, quality of care and quality of life [17], [19]. Three most common use cases where HIE provides benefits are in clinical use, when healthcare providers have access to EHRs that support better treatment-decision making [20]. Secondly, in consumer use when patients have access to their own personal health information (PHI) that informs and engages them as active participants in their health care [20]. And thirdly, using HIE databases to research and analyse this data to support healthcare innovation and improve quality [20].

Although there are a lot of benefits for implementing eHealth services and solutions, the most common barrier for eHealth services integration and adoption is the high cost and the lack of solid evidence of its effects, which unfortunately can lead to key decision makers doubting the effectiveness of eHealth and limiting the investments [19]. Not all eHealth projects are successful and fail to sustain or increase the level of use after the funding ends or there is a lack of healthcare professionals’ willingness to take eHealth systems into use, which again leads organizations to doubt in the cost-effectiveness of their investments [19].

Major challenges in this field are related to the data overload and poor quality [21]. With the rapid rise in the use of EHRs for research the scientists also start to question the quality, reliability and generalizability of this data [22]. The sources of distrust emerge from the limitations of EHRs due to missing or incomplete data for patients who receive healthcare from multiple systems, the errors and incorrect data entered by clinicians, overall inconsistency in data elements across time that is caused by changes in standards, data collection procedures, unstructured data and ability to capture all clinical data [22].

Unfortunately due to human errors, security weaknesses and other vulnerabilities, EHR databases also face the threat of data breaches. These lead to loss or theft of sensitive data because the price of a complete record file of a single patient can be hundreds of dollars on the dark web [22]. In recent years over a 100 million individuals have been affected by these healthcare data breaches [22] that cause serious concerns to both healthcare providers and individuals. And that leads us to another complex challenge that eHealth faces - the balance between patients need for privacy and the need for patient data to improve the efficiency and effectiveness of healthcare [20]. Although it is important to know patient health history when deciding on what treatment to use, then unauthentic internal disclosure and the improper disposal of unnecessary but sensitive data is an internal data breach [23]. Data breaches lead to decrease of trust and restoring that trust can be very expensive money and time wise.

2.5 Digital Transformation

Digital maturity is more often seen in the private sector than in the public sector, but citizens expect that the transactions with their government services are as smooth and high quality as their experience with the private sector, such as online banking or online shopping. The goal of digital transformation is simple – make services so good, that people want to use them, and keep making them better. The way private sector corporations or organizations go through digital transformation towards digital maturity is often replicated in the public sector [24].

One of the key underlying concepts of eHealth is the Digital Transformation (DT) the global healthcare sector is going through at the moment, by having large complex interventions or system implementations that involve major changes to how organizations function [25]. Many researchers claim that healthcare is the main sector or industry where the DT takes place [26], but others state that compared to many sectors, from finance to entertainment, the DT in healthcare still lags behind [27]. According to Walsh and Rumsfeld the main reasons behind this is healthcare being a complex system and it not absorbing innovation as fast because the stakes are high [27]. Matt, Hess and Benlian introduce the DT framework that has four dimensions - use of technologies, changes in value creation, structural changes, and financial aspects. By balancing these four dimensions a DT strategy can be created [28]. The most important part of digital transformation is not technology, but strategy [29].

DT is about increasing productivity, creating value and social welfare, by adopting disruptive technologies. For example DT in software engineering will improve the industry by providing better value-chain integration and new market exploitation with gaining advantages at being more competitive. Concepts that underlie and enable DT are agile development of flexible systems, ensured security and trust in distributed transactions and of course microservices and open Application Programming Interfaces (APIs) that support software architectures [30].

DT is also described as “the profound and accelerating transformation of business activities, processes, competencies, and models to fully leverage the changes and opportunities brought by digital technologies and their impact across society in a strategic and prioritized way” [31]. With this definition the authors describe DT as “accelerating” and “leveraging”. DT creates a more seamless and quicker value-chain than before by enabling us to collaborate and share information. Access to wider knowledge and resources via ICT (smart devices, mobile and cloud computing, big data and analytics and so on) brings us closer to innovation and development [31]. The DT provides means to improve various characteristics of products and services by designing and provisioning new types of service offerings. For example, improving the performance by using automation, improving existing service offerings by changing the service’s traditional production (e.g. telemedicine, online classes, tax software), creating new types of service system coordination through improved value propositions or governance mechanisms (online broker systems, digital health records), integrating customers into service creation and delivery (healthcare information systems, self-service education) and delivering knowledge-intensive professions to labor-intensive employment [31].

According to a survey the biggest barriers for digital transformation is lack of standards, such as international norms, standardized data formats and the lack of compatibility between ports and interfaces [32]. The second biggest barrier is deficiency of skilled workers and know-how, although companies have employees with the right qualification, they lack training concepts, interdisciplinary courses and shortage of young scientists and engineers [32].

A good example of DT in the eHealth domain was the Government Digital Service project in the United Kingdom that was later adopted by Canada, USA, Australia and other countries. These governments are using almost identical set of service standards which were introduced by senior leadership roles that moved from one government digital team to another, spreading the experience and best practices [24]. Digital transformation in healthcare is more complex as the risks are higher because digital healthcare products have potential to harm or kill people and the challenge is to find balance between safety and product design [24]. As the demand for digital health information and services grow, the healthcare sector slowly goes through DT also.

2.6 Technology Acceptance Models

The key element in the process of DT is the continuous use of implemented services or solutions. The ongoing process to ensure user acceptance of technology is an important management challenge [33], because the lack of it can lead to loss of money and resources [34]. IT systems cannot improve organizational performance if they are not used to their full extent or not used at all [35]. The first Technology Acceptance Model (TAM) was developed by Fred D. Davis in 1989, to measure the intention and motivation of users to accept or reject any new technology [36]. TAM has two measures which are: perceived usefulness and perceived ease of use - technologies with a high level of perceived usefulness and perceived ease of use are more likely to be accepted [34]. TAM also has an extension TAM2, and since technologies have improved, there has been numerous adaptations and developments to these models as well.

The unified theory of acceptance and use of technology (UTAUT) was developed in 2003 by analysing TAM, TAM2, Theory of Reasoned Action (TRA), and Diffusion of

Innovation (DOI) in an attempt to attain a unified TAM [37]. UTAUT identifies three direct determinants of behavioural intention to use a technology, such as performance expectancy (degree to which an individual believes that using the system will help him or her better attain significant reward), effort expectancy (degree of ease associated with the use of the system) and social influence (degree to which an individual perceives that important others believe he or she should use the new system) [38]. All these three behavioural intentions are in relation with the user gender, age, experience, and voluntariness [38].

In 2011 Mohamed et al proposed a TAM for eHealth [34] that incorporated additional factors to the original TAM, such as technology design and sociocultural variables (power distance, trust, subjective norm, tangibility, uncertainty avoidance and masculinity). For example in the sample population, trust has a high influence on to use e-Health services and lack of trust will probably increase the intention to use e-Health services [34]. Trust is also one variable of TAM that is considered as an important factor that influences the user's online behaviour and online trust is generated through individual's interactions with online information systems [39].

2.7 Interoperability

As the healthcare systems around the world go through DT, moving from paper-based practices to digital service delivery, then in order to benefit from the opportunities, the underlying keyword here is interoperability. eHealth interoperability is defined as the ability of two or more systems to exchange information [40] in an appropriate and satisfactory manner without the need for extra operator intervention [41]. EHR interoperability enables better workflows, reduces ambiguity [40] and is important for delivering quality healthcare and reducing healthcare costs [41].

Spanakis et al. have proposed an adapted “maturity” model for interoperability in eHealth that consists of five levels that incrementally describe a more mature version of an interoperable infrastructure [42]. First level is non-connected eHealth application where data is held in silos. The second level is a single eHealth application that is directly linked to another application for simple data exchange. On the third level are distributed systems that agree on protocols used, data formats and message exchange patterns. The fourth level is where eHealth applications from different suppliers, that serve a common goal are linked but the applications do not need to have common objectives. The fifth or the universal level is where diverse eHealth applications connect to an open, interoperable infrastructure possibly spanning multiple countries [42]. It seems that most eHealth systems or solutions fall in the first three levels of interoperability. Not too many solutions reach the fourth or fifth level due to the challenges and barriers eHealth brings.

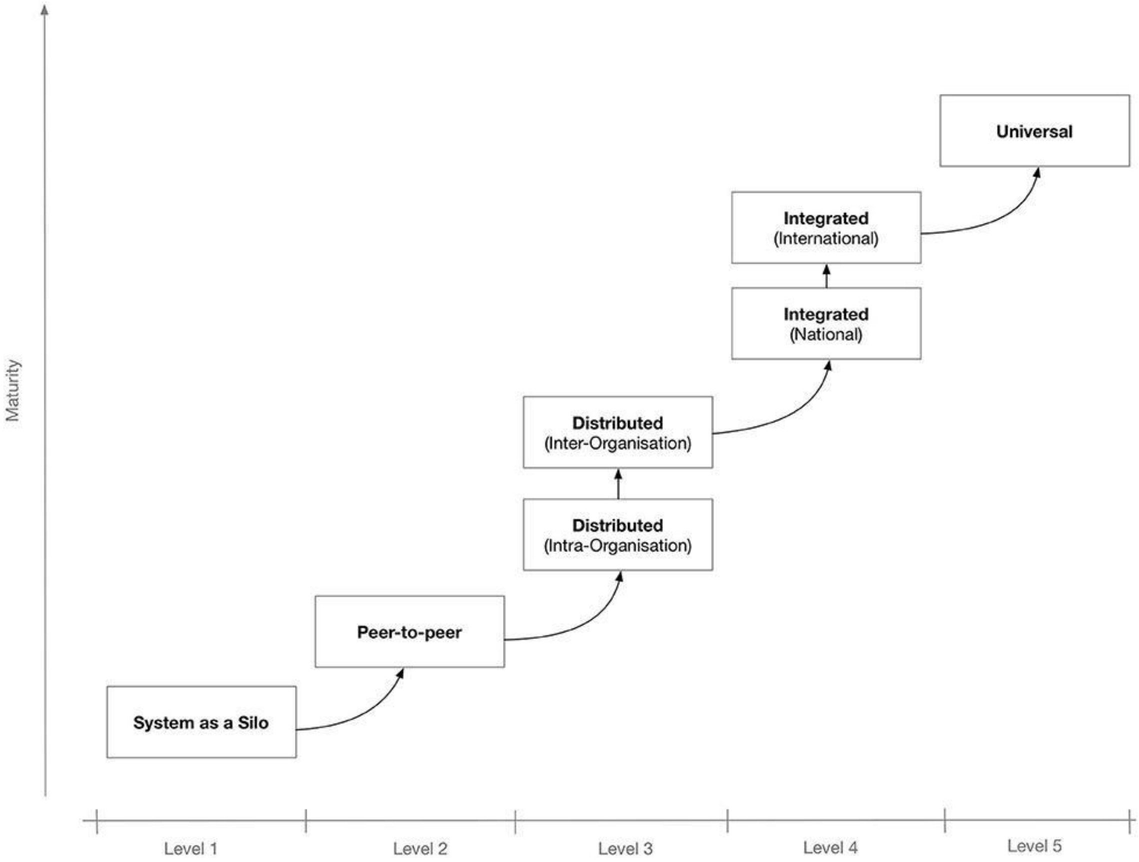

Figure 1. Adapted model of eHealth system interoperability maturity. (Source: Spanakis et al, 2021)

Although the need and importance of eHealth system interoperability is understood and promoted widely [43], achieving it is a challenge due to plethora of competing standards [41], conflicting missions, lack of trust, financing or leadership, data privacy and the high cost of technology [43]. Unfortunately many existing eHealth systems are built in “silos” and lack the ability to interact with each other [44]. These information “silos” are either functional, organizational or technical [44]. According to a Bhartiya et al interoperability usually is weakened due to systems having its own way of representing data, one term having multiple meanings, lack of standard rules for data sharing, lack of integration between different systems that leads to data being in independent silos, data exchange constraints, EHR linking problems and different requirements when exchanging data [40].

Another challenge of interoperability in the healthcare domain is due to the multiplicity of stakeholders such as the patients who are the recipients of the healthcare services, medical professionals that provide the medical care, healthcare organizations who administer the healthcare delivery from a business perspective, insurance companies, pharmaceutical companies who produce and market medications that are used for treatment and last but not least the governments and other regulatory parties who coordinate and set the rules, rights and obligations of all the previously listed stakeholders [42].

2.8 Trust

Davis et al have described trust as "willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" [45]. Being vulnerable means that there is something of importance to be lost and this means there is a willingness to take a risk [45]. In the eHealth domain the "something of importance" is mostly sensitive health data which makes it more vulnerable and the willingness to take risk is lower.

The trust in digital environments and context is called e-trust. There is no direct or physical contact in digital environments as the interactions are mediated by digital devices [46]. Trust in government is defined by OECD as "foundation upon which the legitimacy of public institutions is built and is crucial for maintaining social cohesion and government's values, such as high levels of integrity, fairness and openness of institutions are strong predictors of public trust" [47]. OECD also claims that government's competence is "responsiveness and reliability in delivering public services and anticipating new needs - are crucial for boosting trust in institutions" [47].

Although governments invest a fair amount into e-government development, citizens do not trust e-government systems and are still more likely to use traditional methods instead of digital services [48] [49]. This is due to the increase of data breaches and cases of identity theft, because online frauds and other Internet-related prohibited activities that are now more prevalent than before [49]. Carter and Belanger (2008) claimed that lack of trust hinders the citizen adoption of e-government services and it is imperative that governments acknowledge and invest also in e-government trust issues by budgeting trust-building in addition to technical and staff strategies [50]. The intention to adopt government e-services is mainly predicted by the perceived usefulness of e-services in general, and the latter one is mainly predicted by trust in e-government [51]. Transparency can contribute to trust towards government e-services [48], but here is also research claiming that lack of transparency proves to have no negative effect on trust in government and trust in a government organization is based on a ‘mix of cognition and feeling’ [52].

3 Research Methodology

This chapter describes the chosen design of this research and gives an overview of data sources and explains why these sources were chosen. The research is following qualitative research principles and the methodology for this thesis is exploratory case study and data triangulation.

At the early stages of this research, during the literature overview and attending the weekly meetings with the project team, it became clear that the way cross-border health information is exchanged at the moment, needs major changes. The on-going pandemic gives an opportunity to enforce changes quicker than usual. There is a huge sense of urgency and anticipation to open the global movement of people and return to normalcy again. It started to become clear that current HIE methods and frameworks are fragmented, not interoperable and thus not creating the benefit expected from them. One of the research questions was identified by this discovery. The development of Smart Vaccine Certificates (SVCs) and the need to distribute the health data globally led to the general understanding that a global trust framework is needed to solve this problem. The research gap manifested itself straight away because the "global trust framework" or similar phrases brought almost no Internet search results. With this thesis the author hopes to contribute by providing relevant academic work in the fields of cross-border health data exchange methods and global trust framework.

The data collection methods were participant observation via weekly meetings with international project members, three knowledge-sharing workshops, one semi-structured interview with a technical architect of X-Road based global trust framework and project documentation. As this thesis is interdisciplinary by its nature, the case study research in software engineering is chosen for this research. Case study is one of the most used qualitative research methodologies in many fields of science. Robert Yin is a foundational methodologist in the area of case study design and his suggestions have helped researchers to design their case studies since 2002 [53]. According to Yin, case study is an "empirical inquiry that investigates a contemporary phenomenon in its context, especially when the boundaries between phenomenon and context are not clearly evident" [54]. Robson claims that case study is "a strategy for doing research that involves empirical investigation of a particular contemporary software engineering phenomenon within its real-life context using multiple sources of evidence" [55]. Similarly to Yin, Benbasat mentions a phenomenon with unclear boundaries, but unlike other methodologists, adds that multiple methods of data gathering from one or few entities (people, groups or organization) is employed [56]. According to Yin, a case study strategy is most likely appropriate when "how" and "why" questions need answering [54]. Case studies are considered not only as a formal research method, but a way to observe, explain and explore phenomena in real-life settings [57]. Case study helps to understand why something happened as it did, and what might be important to investigate in future research [57]. Current research also aims to answer research questions of "how" and help to understand the novel case of global trust framework for SVCs by describing the process of composing it.

There are five essential aspects of case study definition - empirical enquiry or investigation, contemporary phenomenon, real-life context, multiple sources and the boundary between phenomenon and context is unclear [58]. The current thesis covers all the essential aspects of previously mentioned case study definition. The phenomenon of global trust framework and SVCs is a novel topic that only recently became discussed and researched. The course of this project changed and evolved sometimes in a few days or weeks while this thesis was written, and until this point the project is not over or finished, which means that real-life context is also present. Multiple sources were used to gather information, starting from weekly meetings to workshops, interview and project documents.

3.1 Data Sources and Collection

Triangulation is a method for increasing the precision and strengthening the validity of a research by having multiple perspectives and providing a broader picture of the researched topic [56]. Data triangulation is defined as "using more than one data source or collecting the same data at different occasions" [56]. For this thesis four sources of evidence have been used - participant observation via weekly meetings with international project members, knowledge-sharing workshops, a semi-structured interview and project related documents.

The author participated in the weekly meetings with the international project team. The aim of these meetings was to exchange information, give an overview of the latest events, discuss action plans in order to achieve the desired goal. The participants were representatives of different state authorities, such as the Government Office, Ministry of Social Affairs, Ministry of Foreign Affairs, Information System Authority (RUA) and Guardtime, the company behind Estonian national SVC solution. In addition to the weekly meetings with project team, the author had also a chance to take part as an observer in meetings with the representatives of other countries who were interested in both – the Estonian national SVC solution VaccineGuard and the global trust framework concept.

Workshops took place with the member of Government Office of Estonia, WHO Digital Health Technical Advisory Group member and field experts from TalTech. The first workshop was attended by eight people, second by four people and third by five people. All three workshops were organized and attended by the author of this thesis. First two workshops took place on spot and all the workshop participants were able to be in the same room and the last one was held online (via MS Teams) because of the ongoing restrictions due to pandemic. These workshops provided a thorough overview of the case background and gave a unique way to see the process unfold and develop as some details of the project got clearer. The goal of these workshops was to firstly get an overview of the project updates, insight information from the project member, to brainstorm ideas and provide academic perspective.

One semi-structured interview was also used, as this is a good choice for exploratory case studies [56]. For semi-structured interview a list of four basic open-ended questions were prepared (Appendix 1) to start the questions, but the interview was not limited to these. The interviewee was the architect of the global trust framework solution proposed by Estonia. The aim of the interview was to get more technical insight to the solution and have one extra point of view to the progress of the case.

Table 1. Data collection methods, data sources and results (Source: Author)

Data collecting methods	Data source	Result

Knowledge-sharing workshops	Member of the Government Office of Estonia, WHO Digital Health Technical Advisory Group member, field experts from TalTech University	In-depth and comprehensive insight to project progress, discussion on barriers, background of decisions, strategic planning
Semi-structured interview	Technical architect of the X-Road based global trust framework	Technical overview of different barriers and alternative solutions
Project documentation	Implementation and project descriptions, memos of the meetings, whitepapers	Specific technical detail description
Weekly meetings with the project team	Project team members from different state authorities and ministries, the company behind Estonian SVC solution	Project overall summary, information sharing between all the authorities and participants, communication planning

3.1.1 Thematic Analysis

In order to analyse the qualitative data, the recordings of three workshops and one interview were transcribed into text by using Otter.ai software that develops speech to text transcription using artificial intelligence and machine learning. Then the author carefully reviewed the software-generated transcripts by comparing them to audio files and corrected all the mistakes and errors that were left in the text. After that transcripts were re-read several times to be familiarized with the data and be sure that no important detail was missing. To analyse the qualitative data gathered from the workshops and interview, thematic analysis method was used, which is one of the most common tools regarding to qualitative content analysis. Braun and Clark have defined thematic analysis as “a method for identifying, analysing and reporting patterns (themes) within data” [59]. A theme is considered to represent some level of patterned response or meaning within the data set [59].

The next steps were to generate initial codes by analysing the whole transcribed data set, then collating codes into themes by grouping the codes. For coding the NVIVO software was used. When the themes were reviewed it became clearer that as this research is in a rapidly evolving and changing phase then based on the research questions the themes were selected accordingly: (1) administrative barriers, (2) legal barriers, (3) technical barriers, (4) trust and (5) opportunities.

Table 2. Phases of thematic analysis (Source: Clark and Brown, 2006)

Phase	**Description of the process**
Familiarizing yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.
Reviewing themes:	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic ‘map’ of the analysis.
Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

4 The Case

The following chapter will give an overview of the Global Trust Framework case background and answer the research question “How is cross-border health data exchanged currently?” and sub-questions “What cross-border health data exchange methods/frameworks are in use?” and “What are the limitations of current health data exchange solutions?” The descriptions of different approaches to Global Trust Framework architecture and SVC pilot implementation are also provided.

4.1 Case Background

2020 and 2021 will be remembered for decades as the years of lockdown, social distancing and extreme pressure on our health systems due to COVID-19 global pandemic. As the borders closed one by one, huge sectors of the economy like transportation and tourism closed down immediately and cancelled millions of work and vacation related trips both locally and internationally. The governments around the globe were under pressure to handle the crisis efficiently, calm the panic, support the struggling economy and steer the society back to pre-pandemic normality. The key element of getting this virus under control was on the shoulders of the pharmaceutical industry - the development of COVID-19 vaccines. In the end of 2020 and beginning of 2021 over 10 different vaccine developers ended their clinical trials and were authorized for use [60]. Additionally a plethora of vaccine candidates were already in different clinical trial phases. When the widespread distribution of vaccines in different parts of the world started, a variety of concerns and problems started to rise as well. Vaccine hesitancy, unequal access to vaccines between high and low income countries and many more topics were discussed as a part of the meetings and workshops, but these are not in the scope of this thesis. As the percentage of the global population that is vaccinated gets higher, the expectations of returning to pre-pandemic life arrangement and mass global travel rise, too. One solution for this might be the SVCs and the central facilitating body of SVC standards and design principles will be WHO. As WHO does not currently have the technical capability for this new role, then as an organization WHO must now undergo digital transformation to be able to facilitate the role as the anchor of trust.

In October 2020, WHO and Estonia signed a Memorandum of Understanding (MoU) to improve the cooperation in the area of digital health and innovation. This MoU was signed in order to collaborate on developing international public health goods and exploring the technologies that improve the health and well-being of populations. The activities and proposed projects in this MoU are for example in the fields of personalized medicine and genomics, standards and leading practices for health data governance and interoperability, ePrescription/eDispensing, global digital health maturity index and European roadmap for the digitalization of health systems. Due to the on-going pandemic, the first project that was focused on, is the development of Digital Certificate of Vaccination or a digital yellow card. The aim of this project is to augment and strengthen the effectiveness of COVAX, and other processes related to vaccination processes, that could be scaled worldwide, including in low-resource settings [61]. As developing interoperable SVC solutions requires a secure and interoperable architecture to exchange data between countries, then one potential data exchange layer would be similar to the X-Road, that is developed and used in Estonia since 2001.

The main responsibility of the WHO has historically been to manage "the global regime for the control of the international spread of disease" [62]. WHO has regulated the International Certificate of Vaccination or Prophylaxis that is also called Yellow Card since 1969 [62]. This certificate is a physical piece of paper that proves being vaccinated against yellow fever and it is still a prerequisite to enter many countries today [63]. Unfortunately forging of these certificates has been a problem for decades [64]. For example, incorrect information about administered vaccines or changing the date of the administration in order to extend the validity of the certification. The reasons behind these falsifications could be anything from the costs of getting a vaccine and certification to vaccine hesitancy. This means that a more secure and trustworthy version of vaccine certifications is required [64].

The Estonian national SVC solution called VaccineGuard is developed by GuardTime, a Europe's leading deep technology company. The product development was based on the collaboration between WHO and the Estonian Government. The underlying technology of VaccineGuard is Keyless Signature Infrastructure (KSI) blockchain [65]. This digital platform connects all the participants of the vaccine ecosystem – the government, the citizen and the manufacturer and by enabling these participants to share data and verify its authenticity across organizational boundaries and international borders, it enables real-time insights, counterfeit detection and many other benefits enabling a faster and reliable pandemic response [66].

In March 2021, two key documents about SVCs were published - one by the European Commission [67] and the other by WHO [68]. These documents both provide definition and guidelines on national SVC design, requirements and the technical specification on global trust framework.

4.2 Current Health Data Exchange standards, methods and frameworks

There is currently a plethora of different methods, standards, frameworks and infrastructures in use for cross-border health data exchange. This section provides an overview of some of the most used ones and answers the research question “How is the cross-border health data exchanged currently?” and sub-questions “What cross-border health data exchange methods/frameworks are in use?” and “What are the limitations of current health data exchange solutions?”

4.2.1 Health Level Seven (HL7)

Health Level Seven International itself is not a standard, but it is a standards creating organization focused on providing a Health Level Seven (HL7) framework for EHR exchange and sharing [69]. These standards define how information is packaged and communicated, what language, structure and data types are required in order to create seamless integration between different systems [70]. The lack of standards is definitely a barrier for EHR implementation [70] and HL7 aims to provide a solution for that. These standards are based on reference information model created to tackle the bottlenecks involved in EHR exchange. Adopting HL7 standards is still a demanding process that requires technical maturity and good knowledge of each concept involved [70] that a lot of countries and medical institutions unfortunately lack, and thus are not able to implement.

4.2.2 District Health Information Software 2 (DHIS2)

District Health Information Software 2 (DHIS2) is an open source, web-based platform that is used as health management information system used by over 70 low and middle-income countries [71]. Health management information systems are not for handling health data records of individuals, but for collecting data for decision-making and information management [72]. It is modular, with layered architecture and an open API that serves as a data warehouse for over 60 native applications [71]. DHIS2 helps to properly analyse the data, provide reports and visualizations to help users make decisions based on this information [72]. The strengths of DHIS2 lie in the flexibility to make changes, which reduces the cost of application preparation and dependence on the software company, but as this software is mainly used in developing countries then the most challenging issue is still the lack of technical knowledge in personnel. These issues lead to problems in implementing and using it [72].

4.2.3 GAIA-X

GAIA-X is a fairly recent framework that originates from the German Federal Government [73] and is focusing on creating an European data infrastructure as a secure federated system with the highest standards of digital sovereignty while promoting innovation [74]. It aims to be an open, transparent digital ecosystem, where data and services can be made available, collated and shared in an environment of trust [74]. This initiative addresses such obstacles as a lack of transparency of data, underlying infrastructure, unclear jurisdiction and the inability to choose between service providers, technology choices and sector-specific data spaces [74]. GAIA-X also promises to reduce dependencies, increase transparency and attractiveness of digital services, and bring together digital infrastructures to foster innovation [75]. The stakeholders in this ecosystem are for example cloud service providers and network providers [73]. As this framework is in quite early stages then it is rather difficult to find any research or reports that would describe the adoption and usage of GAIA-X.

4.2.4 STORK and STORK2.0

Due to huge differences and almost non-existent interoperability between Member States' eID systems, a pilot called STORK (Secure Identity Across Borders Linked) took place from 2008-2011 that aimed to solve these issues [76]. What made this pilot kind of unique was launching it in a real large-scale environment that provided valuable lessons and having end-users testing it [77]. But this project also came with limitations as the scope of this project was scaled down only to natural person authentication in public services, but for comprehensive ecosystem private sector representation is also necessary [77]. To overcome the limitations of the first phase, STORK2.0 was piloted as the second phase of this European Commission project to establish a pan-European authentication framework aimed to build a identity infrastructure by interconnecting existing national systems [77] and therefore creates a single European electronic identification and authentication area [78]. This project is considered overall to be a successful one, as it lead us to implementation of eIDAS in 2018.

4.2.5 eIDAS

In 2018 the EU-wide legislation on the electronic identification (eIDAS Regulation) was introduced that enabled cross-border recognition of the electronic ID that allowed European citizens and businesses to share their identity data when necessary [79]. Electronic IDs (eID) such as ID cards, driver licenses, bank cards can be used across the EU for different services, such as filing tax returns, access medical records and other online public services [79]. In order to recognize every citizen by a member state each country must deploy an eIDAS Node and participate in the trust network [80].

4.2.6 European Union eDelivery

European Union eDelivery network is a project in Connecting Europe Facility programme that provides funding for deployment of digital networks and services to create a European Digital Single Market [81]. eDelivery is a network of nodes for digital communications and it is based on a distributed model where every participant becomes a node using standard transport protocols and security policies [82]. The aim of eDelivery is to enable public administrations to exchange electronic data and documents with other public administrations, businesses and citizens in an interoperable, secure, reliable and trusted way, but as the data is sourced by information systems that are developed independently and, therefore, do not have a common data structure and exchange protocol [83].

4.2.7 The Estonian X-Road

X-Road is defined as “a centrally managed distributed data exchange layer between information systems that provides a standardized and secure way to produce and consume services” [84]. The first version of X-Road was created in Estonia in 2001 and it has since then been the backbone of secure information exchange between private and public sector entities [85]. The use of X-Road is mandatory to governmental institutions by Public Information Act [86]. X-Road is strategically managed and developed by MTÜ Nordic Institute for Interoperability Solutions (NIIS) that is an association that was founded in 2017 by Estonia and Finland [85]. It’s official aim is “to ensure the quality, sustainability, cross-border capability of core e-Government infrastructure components; to save resources upon the development of digital society and cross-border cooperation” [87]. NIIS was created by joining two authorities that previously coordinated the X-Road core development - Finland's Population Register Centre and the Republic of Estonia's Information System Authority [88]. Since X-Road has been implemented in various countries and domains all over the world. For example Iceland adopted X-Road data exchange layer “Straumurinn” at national level in 2018 [89], Germany piloted an electronic portal to manage digital prescriptions in 2020 [90] and many projects are also in production, piloting stage or setup-phase.

4.2.8 Comparison of used methods, frameworks and standards

To answer the research question “How is cross-border health data exchanged currently?” and sub-questions “What cross-border health data exchange methods/frameworks are in use?” and “What are the limitations of current health data exchange solutions?” an overview of used methods, frameworks and standards were given. Based on the overview and their functional descriptions there is currently no single and overarching global method, framework or standard of how health data is currently exchanged. Significant differences between developing and developed countries occur, as the implementation of EHR-related services is knowledge, finance and time consuming, and is therefore unavailable for poorer countries. For example, the HL7 framework is widely used by many countries, but digital maturity and proper finances are barriers for implementing these standards. And as the HL7 provides standards of how health data should be packaged and communicated, then naturally the health data interoperability between countries, who have implemented HL7 standards, and those who have not, is insufficient.

The DHIS2 on the other hand is mostly used in developing countries, but the aim of this software is not exchanging or handling EHRs of individuals, but for collecting data that would benefit decision-making and information management. And as the developed countries are not participants of this data warehouse, then the quality of information is not as high as it could be.

There are also many European programs and projects to enhance the EHR distribution, but these all have their own limitations. These limitations start from not having a common data structure and exchange protocol (eDelivery) [30], each project having its own technical building blocks that are mostly with a domain-specific focus (eProcurement, eHealth and eJustice) [91] and not being therefore suitable for eHealth exchange. eIDAS is a protocol for electronic identifications, that on a citizen level is needed, but again building an efficient and scalable eIDAS infrastructure at the European level requires the integration and harmonisation of several systems, that originally were designed, implemented and maintained by different entities, with different tools and approaches [92]. As the Estonian X-Road is not designed for a specific domain and acts as a secure health data exchange layer, and thus does not exclude any domain or use case, then it could be used for secure global health data exchange, as it is now used on a national level.

4.3 The road to Global Trust Framework

The eHealth Network of the European Union (EU) has defined trust framework for Digital Green Certificate as "the rules, policies, specifications, protocols, data formats and digital infrastructure regulating and allowing for the reliable and secure issuance and verification of certificates to guarantee the certificates' trustworthiness by confirming their authenticity, validity and integrity, including by the possible use of electronic seals" [67]. And the trust framework shall be flexible enough to encompass different use cases, such as both digital and analogue, off-line and on-line versions of the COVID-19 health certificates, as well as the associated verification [67]. But the EU has also claimed that The Digital Green Certificate system is a temporary measure and it will be suspended once the World Health Organization (WHO) declares the end of the COVID-19 international health emergency [93] which means that this is a temporary framework that will be discontinued when the health crisis ends.

WHO on the other hand has added that the design of the global trust framework should “leverage open standards, software global public goods, Open HIE architecture, foundational services, and conformance assessment, to facilitate interoperability, usability, reuse, and quality” [68] which means that other use-cases after SVCs will hopefully follow. It is also stated in this guide that WHO will not become a holder of any personal health data or participate in the verification transactions, but rather the enabler and facilitator of the cross-border interactions between the Member States [68].

4.3.1 The Public Key Directory based Global Trust Framework

One possible architecture for the global trust framework for SVCs is derived from ICAO’s Public Key Directory (PKD) model [94]. The PKD based trust framework relies on a chain of trust between participants and the centrally managed PKD [68]. There is no personal health data stored in the PKD, but a list of public keys that are linked to national public health authorities (PHAs) [68]. PKD itself is a quality-controlled, global master list of public keys, revocation lists and internet endpoints that operationalize the trust network between participants’ PHAs [68]. The management of PKD is the role of trust broker or the anchor of trust that in the case of SVCs is WHO itself.

Thus the PKD based global trust framework is built by establishing public key infrastructures (PKIs) that will create an cryptographically supported trust framework [68]. This that relies on a logic that each country participating in the PKD based global trust framework is responsible for the health data records and issuing SVCs by assigning a national PHA. And the authentication of the person the SVC is issued for is verified by nationally issued identity proof documents [68]. Each Member State is also responsible for establishing and maintaining its own national PKI that should include the highly secure databases for maintaining their private keys and the directories needed to store and manage its own public keys [68].

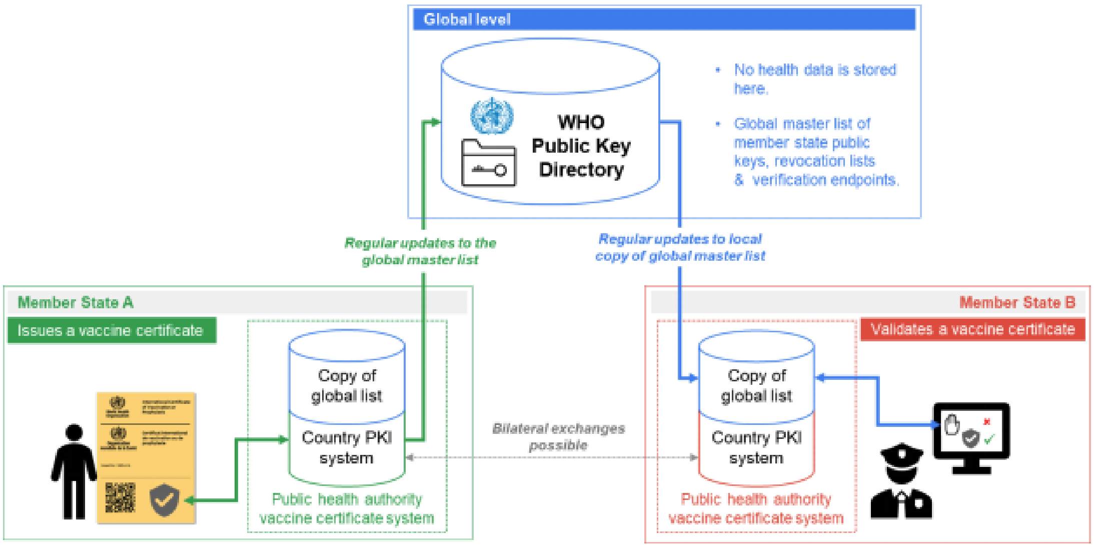
Global level
WHO
Public Key
Directory
No health data is stored here.
Global master list of member state public keys, revocation lists & verification endpoints.
Regular updates to the global master list
Regular updates to local copy of global master list
Member State A
Issues a vaccine certificate
Copy of global list
Country PKI system
Public health authority vaccine certificate system
Bilateral exchanges possible
Member State B
Validates a vaccine certificate
Copy of global list
Country PKI system
Public health authority vaccine certificate system

Figure 2. PKD-based global trust framework architecture. (Source: WHO)

4.3.2 The X-Road based Global Trust Framework

An alternative solution to the PKD-based global trust architecture approach was proposed by the Government of Estonia. The technical solution for piloting will be X-Road, which is an open-source, free of charge software and ecosystem solution that provides unified and secure data exchange between organisations [95]. The secure X-Road global trust framework's fundamental principle is that "one can trust the data when it originates from the trusted source and can have a legal effect" [95]. This means that this framework is data-independent and the main emphasis is on identifying the data provider, not the data itself - if one trusts the data origin country, then one can trust the source that provides the data and thus one can trust the data itself.

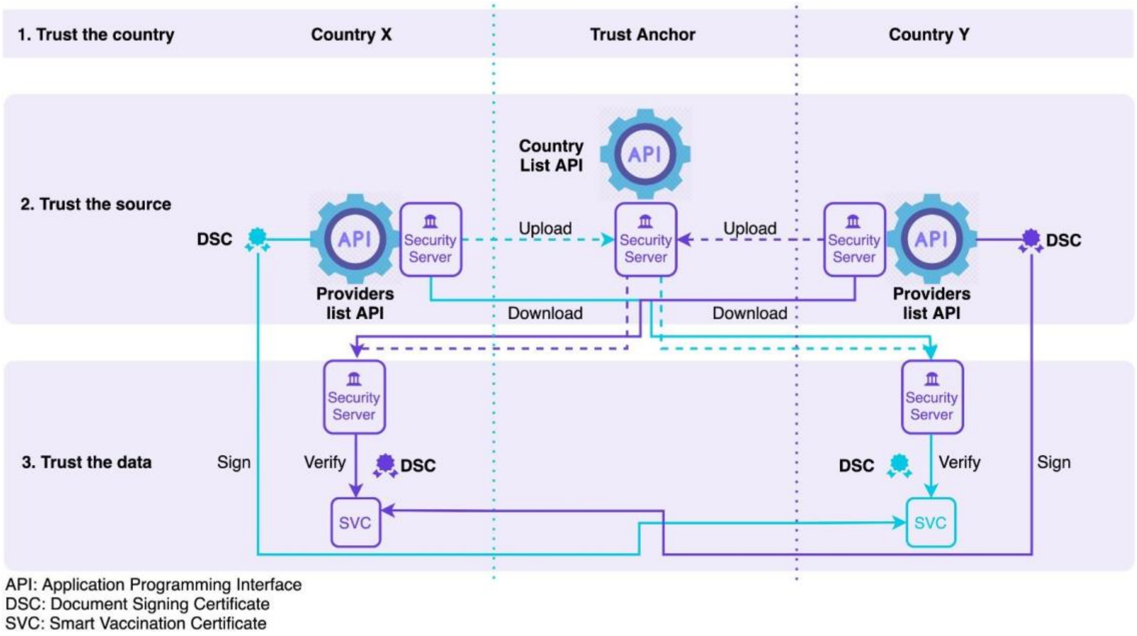

Figure 3. Three layers of trust. (Source: project documents)

In both cases (The X-Road based and PKD-based global trust framework) the role of WHO will be the same - to be the global anchor of trust. The biggest challenge for WHO is to build capacity inside the organization in order to be able to manage the global master list of 194 Member states.

Initial piloting deployment of the global trust framework may focus on less sensitive data and standardised data services that will provide relief to the current crisis. This means that no sensitive health data is exchanged regarding the SVCs, but the exchanged data consists of public keys, Certificate Revocation Lists and other metadata [95]. As this data is the foundation of trust for SVCs, it is important to ensure its authenticity and integrity [95].

As members of the global trust framework will exchange data directly and securely, it will also allow the transfer of delicate health data if required. In this solution, every member of the framework is in full power to enable and disable the access rights only to the selected organisations.[98] Each participating country is free to choose their processes and solutions on how and to whom they provide the data and how they act on the received data. The global trust framework must provide organizational and technological solutions on how to identify the trusted sources and exchange data securely.

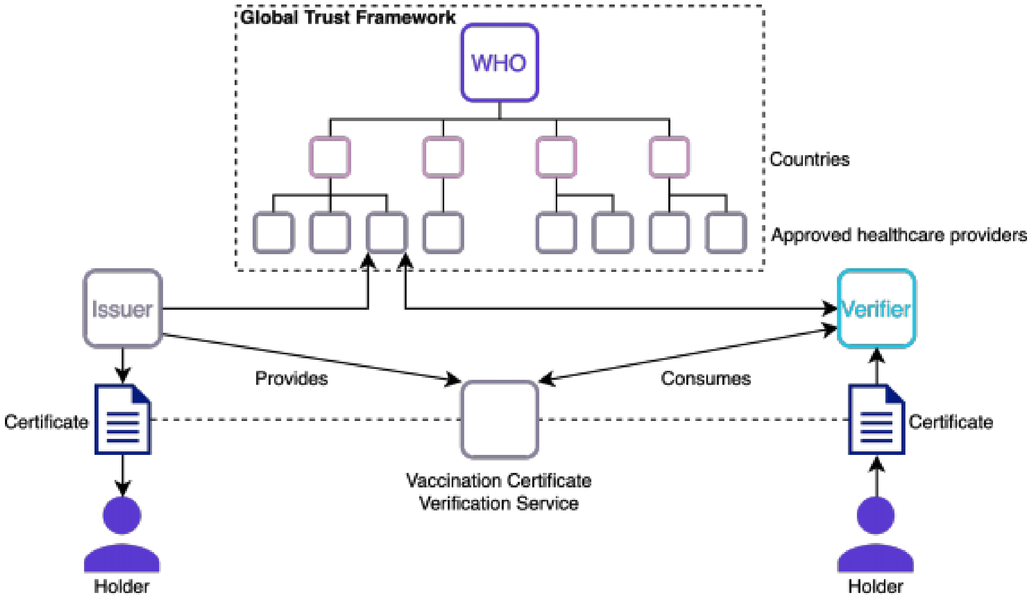

Figure 4. Global trust framework for SVCs. (Source: project documentation)

5 Discussion

In this section the results of the research will be discussed. The author will present the conclusions and also the limitations of the research.

During the course of this project there were quite a few “pivotal” moments where seen obstacles and problems resolved quicker than expected – for example the WHO not having the mandate to run the SVC program or act as the anchor of trust for global trust framework. The initial plan was to wait for the annual WHA in May 2021, due to the urgency of this case, the leadership of WHO made decision in March 2021. This means that WHO took a clear step towards the digital society and start offering a practical service to its member states. But there were also obstacles that were not anticipated, for example based on meetings and discussion with WHO, the project team was under the impression that the global trust framework that is going to be endorsed by WHO is based on X-Road architecture. But in March 2021 when the European Union and WHO published the documents that gave guidelines for developing national SVCs, the chosen solution was is based on the ICAO’s PKD solution.

One of the arguments against the PKD approach is that it would fail to achieve the goals it was set to achieve - to be the global public good and have the capacity of scaling to other medical use-cases in the future. But the biggest critique for PKD-based framework is that as the deployment price of the PKD-based framework is too high for many low and middle resource settings and the digital skills and capacity of public health officials does not meet the requirements, this creates a huge inequality between developed and developing countries. It is also noted that this approach would technically scale to global needs with SVCs, but it would be difficult to scale to future eHealth related use-cases. And this should not be mixed with critique against engineering and PKD-approach itself, but rather it is not adequate for the case of Smart Vaccine Certificates, because model requires every government to set up healthcare domain National PKDs and Certificates Authorities (CA) enabling the SVCs based Public Key Infrastructure (PKI).

Based on the previous critique for PKD based solution, the project team still decided to continue with piloting the X-Road based solution as in the longer run when SVCs use case is not needed or the solution fails, this would be piloted, tested and ready for deployment to production. As there has not been any global trust framework implemented during the writing of this thesis and, then the focus will be on API-based approach, similar to the X-Road we have in Estonia.

5.1 Summary of Findings

The data triangulation between literature review, knowledge-sharing workshops, semi-structured interview, project documentation and weekly meetings with the project team were used for this research. The research itself is qualitative by its nature and the used method is case study. These sources were chosen because of their involvement and knowledge of the chosen project. The conducted workshops and an interview were recorded, transcribed and coded. The analysis of the findings is based on these outcomes.

The findings helped to answer the research questions mentioned at the beginning of the thesis. The first research question was “How is cross-border health data exchanged currently?” It aimed to describe the current cross-border health data exchange methods and their weaknesses. In order to achieve the aimed result, following sub-questions were addressed - “What cross-border health data exchange methods/frameworks are in use?” and “What are the limitations of current health data exchange solutions?” This research question and sub-questions were discussed and answered in Chapter 4.2.

The second research question was “How can X-Road based Global Trust Framework be implemented for Smart Vaccine Certificates?” and for answering that, the sub-question “What are the legal, administrative and technological barriers for implementing global trust framework?” was asked. The answer to the sub-question helps to identify the barriers that are needed to overcome in order to implement the global trust framework for SVCs.

It was mentioned several times during the interview and workshops that the ongoing crisis has created a unique moment for implementing a global trust framework. The sense of urgency allows to skip the long bureaucratic process of creating rules, standards, and so on. When time constraints are strict, then fast decisions are needed, but even in this case there are barriers that must be overcome in order to implement any new solutions.

Administrative barriers

The administrative barriers are mostly related to WHO historically not being in charge of technical aspects of eHealth. WHO by nature is a science-based organization that mainly focuses on creating standards and norms. In the case of global pandemic, WHO is now taking up the role of the anchor of trust in the global trust framework. This means that WHO must undergo a digital transformation in order to overcome their current lack of technical competence. They do not currently have prior experience similar to this case. Moreover, the WHA takes place only once a year, which is needed to change the IHR that at the moment does not give WHO a mandate to run this framework and be the anchor of trust.

Legal barriers

The biggest legal barriers are IHR constraints for WHO to take the role of global trust anchor. IHR states that WHO has mandate only for Yellow card that needs handwritten signatures from doctors and does not give WHO mandate to run global trust framework. On a more broader level it is needed for WHO in order to get global trust framework running to get all the 195 countries legally binded. Laws and norms always take time to get enforced, and while they do, the real life is again few steps ahead. In the case of SVCs, one legal problem is that 1 billion people on the planet lack any sort of identity, meaning that linking a person with SVC is currently not possible and 3,5 billion people don't have biometrical passports that is necessary for a PKD-based solution. Furthermore, there are many countries that lack any sort of governance and are considered to be failed states.

Technical barriers

Amongst the technical barriers, the biggest challenge for implementing trust framework is the lack of national SVCs. It also seems that most negotiations on any new and novel solutions start from the technical questions, but it should be the other way around – to get the administrative, legal and, for example, trust details sorted. Only after that head on to more technical questions. As a barrier it is mentioned that one issue for X-road based trust framework is competing solutions, namely the PKI-based trust framework, that is based on biometrical passports. As brought out in the legal barrier section, there are over 1 billion people, who lack any sort of identity and 3,5 billion people who lack biometrical passports. A PKD-based solution requires setting up a national Certificate Authority, that is expensive, time consuming and therefore unavailable for many developing countries. And a PKD-based solution is usable only for the SVC use case and is not scalable for other use cases.

Opportunities

Whenever there are barriers there also are opportunities of overcoming these obstacles. When it was brought out during the workshop and the interview, that WHO lacks technical competency, then the MoU signed between WHO and Estonia can be considered as an opportunity to cooperate on a technical level. Since Estonia has developed the data exchange layer X-Road it could very well be suitable for a global SVC exchange and possibly for other use cases as well. It was also brought out during the workshops that there are many failed state countries where organizations such as Doctors Without Borders or Red Cross could take upon themselves the role of the anchor of trust.

Trust

Trust was mentioned during the workshops as the key foundation and a basis of any initiative that involves cooperation and exchange of data. The way the workshop participants perceived trust is that transparent communication is the groundwork of a trustable service that should be discussed before any other topics, such as the choice of technology. Recently the WHO also published the global eHealth strategy and one of the key deliverables was also trust.

The second research question was “How can X-Road based Global Trust Framework be implemented for Smart Vaccine Certificates?” and the sub-question was “What are the legal, administrative and technological barriers for implementing global trust framework?” Based on the interview outcomes, the key strategy was to first find the barriers that this project might face – these were identified as technical, legal and administrative barriers. During the course of this project, many of them were removed thanks to the urgency of this case - for example the WHO’s mandate to run the global trust framework and act as the anchor of trust. Many barriers occurred to the team during, that were not considered as a barrier or risk before – such as alternative solutions for the global trust framework. And after these barriers were identified, then overcome and match them with opportunities, that could lower or erase the barrier. For example, as WHO has historically been a standards creating body and now needs to take up this new technically demanding role, the opportunity was to sign a MoU with a Estonia, who is known for its ambitious and well-working projects, such as the X-Road or eResidency. And it was mentioned several times during these workshops and interview, that the SVC pilot is only the beginning – there are many beneficial use-cases waiting for piloting and implementing.

5.2 Limitations

The limitations of this research are on one hand related to the subjectivity of the workshop participants and the interviewee. They were all the representatives and supporters of the X-Road based solution, but the viewpoints of the WHO and PKD-based solution provider would give this research more depth and understanding why some decisions were made in a certain way. As the project is still unfinished, no solution has been deployed, then it is also impossible to draw conclusions of the successfulness and effectiveness of the global trust framework pilot for SVCs.

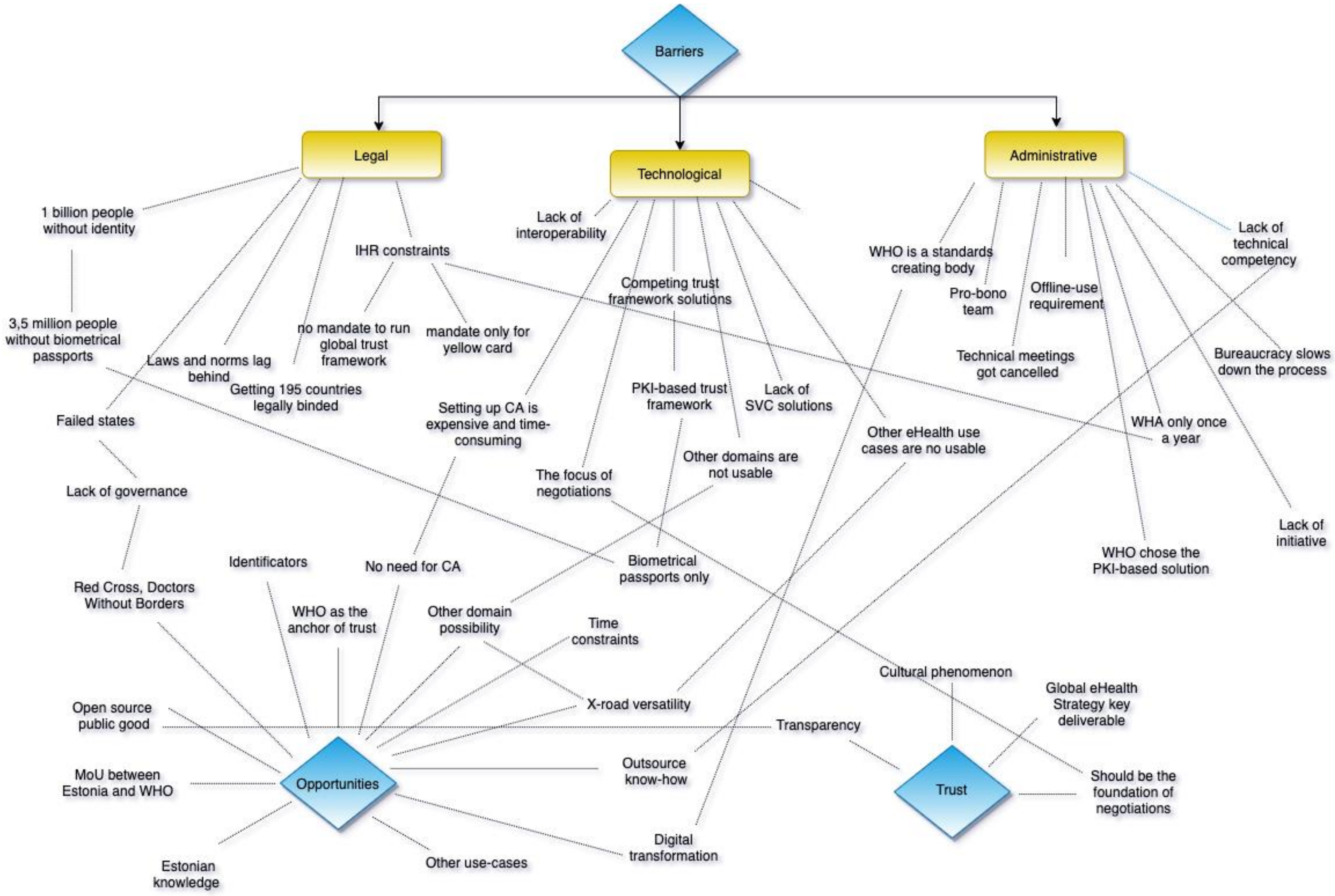
Barriers
Legal
Technological
Administrative
1 billion people without identity
3,5 million people without biometrical passports
Laws and norms lag behind
IHR constraints
no mandate to run global trust framework
mandate only for yellow card
Getting 195 countries legally binded
Failed states
Lack of governance
Red Cross, Doctors Without Borders
Lack of interoperability
Competing trust framework solutions
PKI-based trust framework
Lack of SVC solutions
Setting up CA is expensive and time-consuming
The focus of negotiations
Other domains are not usable
Other eHealth use cases are no usable
Biometrical passports only
WHO is a standards creating body
Pro-bono team
Offline-use requirement
Lack of technical competency
Technical meetings got cancelled
Bureaucracy slows down the process
WHA only once a year
WHO chose the PKI-based solution
Lack of initiative
Identificators
No need for CA
WHO as the anchor of trust
Other domain possibility
Time constraints
X-road versatility
Open source public good
Transparency
MoU between Estonia and WHO
Opportunities
Outsource know-how
Estonian knowledge
Other use-cases
Digital transformation
Cultural phenomenon
Global eHealth Strategy key deliverable
Trust
Should be the foundation of negotiations

Figure 5. Thematic map (Source: Author)

5.3 Conclusions

In order to open up the global free movement and limit the potential spread of the COVID-19 virus, the need and anticipation for Smart Vaccine Certificates was raised. And as an important cornerstone for exchanging SVCs is the Global Trust Framework that acts as a secure data exchange method. As the WHO has historically been a humanitarian and standards creating body, then a Memorandum of Understanding was signed with Estonia who is known for its X-Road and many other eGovernment projects. The collaboration and cooperation would be in the area of digital health and innovation. As developing interoperable solutions requires a secure and interoperable architecture to exchange data between countries, then one potential global trust framework solution could be the Estonian data exchange layer X-Road, that is developed and used in Estonia since 2001. The first piloting phase case of SVCs is important to create trust and prove the efficiency of this solution and to discover the legal, administrative and technical implementation barriers, opportunities and necessary amendments before fully deploying this solution to production.

The author of this paper participated in the project team meetings, had three knowledge-sharing workshops, one interview and had access to project documents. During the process of this research case unfolded in front of all the participants in this project, changed course and forced the project team to readjust objectives and plans. All the usual steps in creating a global standard happened at a much faster pace due to the ongoing global pandemic.

Two research questions, with sub-questions, were asked at the beginning of this research, the first being “How is cross-border health data exchanged currently?” and “How can X-Road based Global Trust Framework be implemented for Smart Vaccine Certificates?” To answer the first question, the existing methods, frameworks and standards that are used at the moment to exchange health data were described and analyzed. As an outcome it was clear that firstly there is a huge gap between developing and developed countries, as the implementation of most solutions is difficult and financially burdening. But on the other hand, the solutions that are implemented in the developing countries are not used by developed countries. And on the European level there are also many programs, data exchange frameworks, but most of them are domain-specific or suitable for exchanging eHealth data. The second question was answered by identifying the barriers and opportunities that would be needed to overcome these. Barriers were identified by thematic analysis and coding, that mapped out three main areas – administrative, legal and technical barriers. The biggest administrative barriers were the technical incompetency of the WHO, that were challenged by the opportunity of collaborating with Estonia, who is experienced and has existing solutions in production already. The legal barriers entailed the IHR constraints, but this was actually solved due to the urgency of this case. The biggest technical barrier was at the beginning of this research the lack of SVCs for piloting, but as things progressed, at one point it got clear that WHO decided to endorse an alternative solution for global trust framework. As the competing PKD-based solution was described, it was also clear that this PKD-based solution is not meant for alternative use cases after SCVs. Based on that the project team will also continue with the X-Road based global trust framework pilot for SVCs model, as this is more versatile and could be scaled for other use cases in the future.

5.4 Future work

Global trust framework is a concept that has never been implemented before, thus there are a lot of areas that could be researched in the future. The first would be to analyse the actual global trust framework pilots for SVCs in action, both PKD-based and X-Road based solutions. Then a comparative research between the actual implementation cost, time, ease of these solutions for both developing and developed countries. These research areas will give the WHO and the Member States very insightful information on the topic. And as the next step to for this project is to implement global trust framework for next uses cases, then the future work seems quite endless at the moment, because SVCs is only small fraction of eHealth data that needs to be exchanged between countries.

References

[1] Ministry of Foreign Affairs, “Digital health and innovation cooperation with the World Health Organization (WHO) on the Smart Vaccination Certificate,” [Online]. Available: https://vm.ee/en/digital-health-and-innovation-cooperation-world-health-organization-who-smart-vaccination. [Accessed 8 May 2021].

[2] I. Pappel, V. Tsap and D. Draheim, “Exploring e-Services Development in Local Government Authorities by Means of Electronic Document Management Systems,” *Electronic Governance and Open Society: Challenges in Eurasia,* vol. 947, pp. 223-234, 2019.

[3] I. Pappel, V. Tsap and D. Draheim, “The e-LocGov Model for Introducing e-Governance into Local Governments: an Estonian Case Study,” *IEEE Transactions on Emerging Topics in Computing,* 2019.

[4] J. D. Twizeyimana and A. Andersson, “The public value of E-Government – A literature review,,” *Government Information Quarterly,* vol. 36, no. 2, 2019.

[5] T. Kalvet and A. Aaviksoo, “The Development of eServices in an Enlarged EU: eGovernment and eHealth in Estonia,” European Commission, Luxembourg , 2008.

[6] J. Rowley, “e-Government stakeholders—Who are they and what do they want?,” *International Journal of Information Management,* vol. 31, no. 1, pp. 53-62, 2011.

[7] WHO, “Global Observatory for eHealth,” [Online]. Available: https://www.who.int/observatories/global-observatory-for-ehealth. [Accessed 9 May 2021].

[8] H. C. Ossebaard and L. V. Gemert-Pijnen, “eHealth and quality in health care: implementation time,” *International Journal for Quality in Health Care,* vol. 28, no. 3, p. 415–419, 2016.

[9] S. Al-Sharhan, E. Omran and a. K. Lari, “An integrated holistic model for an eHealth system: A national implementation approach and a new cloud-based security model,” *International Journal of Information Management,* vol. 47, p. 121–130, 2019.

[10 European Commission, “EHR, the core component of eHealth,” 2010. [Online]. Available: https://joinup.ec.europa.eu/collection/ehealth/document/ehr-core-component-ehealth. [Accessed 9 May 2021].

[11 A. A, S. A and P. C, “Health Information Exchange as a Complex and Adaptive Construct: Scoping Review,” *Journal of Innovation in Health Informatics,* vol. 23, no. 4, p. 633–683, 2016.

[12 R. Haux, “Health information systems – past, present, future,” *International Journal of Medical Informatics,* vol. 75, no. 3, pp. 268-281, 2006.

[13 WHO, “World Health Assembly,” [Online]. Available: https://www.who.int/about/governance/world-health-assembly. [Accessed 2021 May 9].

[14 WHO, “The Fifty-eighth World Health Assembly - eHealth,” [Online]. Available: https://apps.who.int/iris/bitstream/handle/10665/20378/WHA58_28-en.pdf;jsessionid=2E99142B31B0FBEE98C2772088CE863F?sequence=1. [Accessed 9 May 2021].

[15 R. Joosten, D. Whitehouse and P. Duquenoy, “Putting identifiers in the context of eHealth: introduction of a model,” *International Federation for Information Processing Digital Library; The Future of Identity in the Information Society,* 2021.

[16 Official Journal of the European Union, “Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare,” 4 April 2011. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2011/24/oj. [Accessed 9 May 2021].

[17 European Commission, “eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century,” 5 12 2012. [Online]. Available: https://ec.europa.eu/health/sites/default/files/ehealth/docs/com_2012_736_en.pdf. [Accessed 9 May 2021].

[18 D. Whitehouse, C. George and P. Duquenoy, “Global Telemedicine and eHealth Updates: Knowledge Resources,” in *eHealth: legal, ethical and governance challenges - an overview* , International Society for Telemedicine & eHealth (ISfTeH) , 2011, pp. 423-428.

[19 T. Bergmo, “How to Measure Costs and Benefits of eHealth Interventions: An Overview of Methods and Frameworks,” *Journal of Medical Internet Research,* vol. 17, no. 11, 2015.

[20 N. Shen, T. Bernier, L. Sequeira, J. Strauss, M. Pannor Silver, A. Carter-Langford and D. Wiljer, “Understanding the patient privacy perspective on health information exchange: A systematic review,” *International Journal of Medical Informatics,* vol. 125, pp. 1-12, 2019.

[21 I. Noreña, N. Shah, J. Ndenkeh and e. al., “eHealth: Trends and innovations,” in *CIHLMU Symposium 2020,* 2020.

[22 S. T. Savitz, L. A. Savitz, N. S. Fleming, N. D. Shah and A. S. Go, “How much can we trust electronic health record data?,” *Healthcare,* vol. 8, no. 3, 2020.

[23 A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar and R. A. Khan, “Healthcare Data Breaches: Insights and Implications,” *Healthcare,* vol. 8(2), no. 133, 2020.

[24 K. Benjamin and H. Potts, “Digital transformation in government: Lessons for digital health?,” *Digital Health,* vol. 3, no. 1-5, 2018.

[25 A. Burton-Jones, S. Akhlaghpour, S. Ayre, P. Barde, A. Staib and C. Sullivan, “Changing the conversation on evaluating digital transformation in healthcare: Insights from an institutional analysis,,” *Information and Organization,* vol. 30, no. 1, 2020.

[26 S. Kraus, F. Schiavone, A. Pluzhnikova and A. C. Invernizzi, “Digital transformation in healthcare: Analyzing the current state-of-research,” *Journal of Business Research,* vol. 123, pp. 557-567, 2021.

[27 M. N. Walsh and J. S. Rumsfeld, “Leading the Digital Transformation of Healthcare: The ACC Innovation Strategy,” *Journal of the American College of Cardiology,* vol. 70, no. 21, pp. 2719-2722, 2017.

[28 C. Matt, T. Hess and A. Benlian, “Digital Transformation Strategies,” *Business & Information Systems Engineering,* vol. 57, p. 339–343, 2015.

[29 G. K. Kane, D. Palmer, A. N. Phillips, D. Kiron and N. Buckley, “Strategy, Not Technology, Drives Digital Transformation,” 14 July 2015. [Online]. Available: https://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/https://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/. [Accessed 9 May 2021].

[30 C. Ebert and C. H. C. Duarte, “Digital Transformation,” *IEEE Software* , vol. 35, no. 4, pp. 16-21, 2018.

[31 H. Demirkan, J. C. Spohrer and J. J. Welser, “Digital Innovation and Strategic Transformation,” *IT Pro,* vol. November/December, pp. 14-18, 2016.

[32 R. Glass, A. Meißner, C. Gebauer, S. Stürmer and J. Metternich, “Identifying the barriers to Industrie 4.0,” *Procedia CIRP* , vol. 72, pp. 985-988, 2018.

[33 M. Williams, N. Rana and Y. Dwivedi, “The unified theory of acceptance and use of technology (UTAUT): a literature review,” *Journal of Enterprise Information Management,* vol. 28, no. 3, pp. 443-488, 2015.

[34 A. H. H. M. Mohamed, H. Tawfik, L. Norton and D. Al-Jumeily, “e-HTAM: A Technology Acceptance Model for electronic health,” in *nternational Conference on Innovations in Information Technology,* 2011.

[35 F. D. Davis, B. R. P. and P. R. Warshaw, “User Acceptance of Computer Technology: A Comparison of Two Theoretical Models,” *Management Science,* vol. 35, no. 8, 1989.

[36 D. Davis, “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology,” *MIS Quarterly,* vol. 13, no. 3, pp. 319-340 , 1989.

[37 C. Jacob, A. Sanchez-Vazquez and C. Ivory, “Understanding Clinicians’ Adoption of Mobile Health Tools: A Qualitative Review of the Most Used Frameworks,” *JMIR mHealth and uHealth,* vol. 8, no. 7, 2020.

[38 V. Venkatesh and X. Zhang, “Unified Theory of Acceptance and Use of Technology: U.S. Vs. China,” *Journal of Global Information Technology Management,* vol. 13, no. 1, pp. 5-27, 2010.

[39 K. Wu, Y. Zhao, Q. Zhu, X. Tan and H. Zheng, “A meta-analysis of the impact of trust on technology acceptance model: Investigation of moderating influence of subject and context type,” *International Journal of Information Management,* vol. 31, no. 6, pp. 572-581, 2011.

[40 S. Bhartiya and D. Mehrotra, “Exploring Interoperability Approaches and Challenges in Healthcare Data Exchange,” vol. 8040, pp. 52-65, 2013.

[41 A. Dogac, “Interoperability in eHealth systems,” *VLDB Endowment,* vol. 5, no. 12, 2012.

[42 E. G. Spanakis, S. Sfakianakis, S. Bonom, C. C., S. Magalini and V. Sakkalis, “Emerging and Established Trends to Support Secure Health Information Exchange,” *Frontiers in Digital Health,* vol. 3, 2021.

[43 C. Sicotte and G. Pare, “Success in health information exchange projects: Solving the implementation puzzle,” *Social Science & Medicine,* vol. 79, no. 8, pp. 1159-1165, 2010.

[44 J. Weber-Jahnke, L. Peyton and T. Topaloglou, “eHealth system interoperability,” *Information Systems Frontiers,* vol. 14, no. 1-3, 2012.

[45 R. C. Mayer, J. H. Davis and F. D. Schoorman, “An Integrative Model of Organizational Trust,” *The Academy of Management Review,* vol. 20, no. 3, pp. 709-734, 1995.

[46 M. Taddeo, “Defining Trust and E-trust: Old Theories and New Problems,” [Online]. Available: https://www.academia.edu/1505535/Defining_Trust_and_E_trust_Old_Theories_and_New_Problems. [Accessed 9 May 2021].

[47 OECD, “Trust in Government,” [Online]. Available: https://www.oecd.org/gov/trust-in-government.htm. [Accessed 9 May 2021].

[48 A. Lee and Y. Levy, “The effect of information quality on trust in e-government systems ' transformation,” *Transforming Government: People, Process and Policy,* vol. 8, no. 1, pp. 76-100, 2014.

[49 D. Belanche, L. V. Casaló, C. Flavián and J. Schepers, “Trust transfer in the continued usage of public e-services,” *Information & Management,* vol. 51, no. 6, pp. 627-640, 2014.

[50 F. Bélanger and L. Carter, “Trust and risk in e-government adoption,” *The Journal of Strategic Information Systems,* vol. 17, no. 2, pp. 165-176, 2008.

[51 M. Horst, M. Kuttschreuter and J. M. Gutteling, “Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands,” *Computers in Human Behavior,* vol. 23, no. 4, pp. 1838-1852, 2007.

[52 S. Grimmelikhuijsen, “Linking transparency, knowledge and citizen trust in government: an experiment,” *International Review of Administrative Sciences* , vol. 78, no. 1, pp. 50-73, 2012.

[53 B. Yazan, “Three Approaches to Case Study Methods in Education: Yin, Merriam, and Stake,” *The Qualitative Report,* vol. 20, no. 2, 2015.

[54 R. K. Yin, Case study research design and methods (5th ed.), SAGE Publications, 2003.

[55 C. Robson, “Real World Research : A Resource for Social Scientists and Practitioner-Researchers,” 2002.

[56 P. Runeson, M. Höst, A. Rainer and B. Regnell, Case Study Research in Software Engineering : Guidelines and Examples,, John Wiley & Sons, Inc. , 2012.

[57 J. M. Verner, J. Sampson, V. Tosic, N. A. A. Bakar and B. A. Kitchenham, “Guidelines for industrially-based multiple case studies in software engineering,” *2009 Third International Conference on Research Challenges in Information Science,* pp. 313-324, 2009.

[58 C. Wohlin, “Case Study Research in Software Engineering—It is a Case, and it is a Study, but is it a Case Study?,” *Information and Software Technology,* vol. 122, 2021.

[59 V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qualitative Research in Psychology,* pp. 77-101, 2008.

[60 T. Le, Z. Andreadakis, A. Kumar, R. G. Roman, S. Tollefsen, M. Saville and S. Mayhew, “The COVID-19 vaccine development landscape,” 9 April 2020. [Online]. Available: https://www.nature.com/articles/d41573-020-00073-5.

[61 Ministry of Foreign Affairs, “Memorandum of Understanding between The World Health Organization (WHO) and The Government of the Republic of Estonia,” 2020. [Online]. Available: https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/who_estonia_mou_05.10.2020.pdf. [Accessed 9 May 2021].

[62 WHO, “INTERNATIONAL HEALTH REGULATIONS (2005). THIRD EDITION.,” 2005. [Online]. Available: https://apps.who.int/iris/bitstream/handle/10665/246107/9789241580496-eng.pdf?sequence=1&isAllowed=y. [Accessed 9 May 2021].

[63 WHO, “List of countries, territories and areas - Yellow fever vaccination,” [Online]. Available: https://www.who.int/ith/ith_country_list.pdf. [Accessed 9 May 2021].

[64 P. Adepoju, “The yellow fever vaccination certificate loophole in Nigeria,” vol. 394, no. 10194, pp. 203-204, 2019.

[65 Guardtime Health, “VaccineGuard - Whitepaper,” January 2021. [Online]. Available: https://m.guardtime.com/files/Guardtime_VaccineGuard_Whitepaper_v2.pdf. [Accessed 9 May 2021].

[66 Guardtime, “VACCINEGUARD - END TO END VISIBILITY FOR THE PHARMACEUTICAL VALUE CHAIN,” [Online]. Available: https://guardtime.com/vaccineguard. [Accessed 9 May 2021].

[67 European Commission, “Proposal for a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate),” 17 March 2021. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:38de66f4-8807-11eb-ac4c-01aa75ed71a1.0024.02/DOC_1&format=PDF. [Accessed 9 May 2021].

[68 WHO, “Interim guidance for developing a Smart Vaccination Certificate,” 19 March 2021. [Online]. Available: https://cdn.who.int/media/docs/default-source/documents/interim-guidance-svc_20210319_final.pdf?sfvrsn=b95db77d_11. [Accessed 9 May 2021].

[69 HL7, “About HL7,” [Online]. Available: https://www.hl7.org/index.cfm. [Accessed 9 May 2021].

[70 T. Viangteeravat, M. N. Anyanwu, V. R. Nagisetty, E. Kuscu, M. E. Sakauye and D. Wu, “Clinical data integration of distributed data sources using Health Level Seven (HL7) v3-RIM mapping,” *Journal of Clinical Bioinformatics,* vol. 2, no. 2, p. 32, 2011.

[71 DHIS2 , “About DHIS2,” [Online]. Available: https://dhis2.org/about/. [Accessed 9 May 2021].

[72 D. R, H. A, K. A, H. F, R. H, P. A, K. N, K. Z, M. N, H. M, R. S, H. H, M. MH, K. E and A. S., “The District Health Information System (DHIS2): A literature review and meta-synthesis of its strengths and operational challenges based on the experiences of 11 countries,” *Health Information Management,* vol. 48, no. 2, pp. 62-75, 2019.

[73 A. Braud, G. Fromentoux, B. Radier and O. Le Grand, “The Road to European Digital Sovereignty with Gaia-X and IDSA,” *IEEE Network,* vol. 35, no. 2, pp. 4-5, 2021.

[74 GAIA-X, “GAIA-X: A Federated Data Infrastructure for Europe,” [Online]. Available: https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Dossier/gaia-x.html. [Accessed 9 May 2021].

[75 GAIA-X, “GAIA-X: Driver of digital innovation in Europe,” May 2020. [Online]. Available: https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-driver-of-digital-innovation-in-europe.pdf?__blob=publicationFile&v=8. [Accessed 9 May 2021].

[76 Estonian Centre of Registers and Information Systems, “For a Secure Electronic Tool on Cross-Border Electronic Transmission of Certified Copies of Wills,” Tallinn, 2016.

[77 C. Ribeiro, H. Leitold, S. Esposito and D. Mitzam, “STORK: a real, heterogeneous, large-scale eID management system,” *International Journal of Information Security,* vol. 17, no. 5, p. 569–585, 2018.

[78 European Union, “STORK 2.0 - Secure idenTity acrOss boRders linKed 2.0 (STORK 2.0),” [Online]. Available: https://joinup.ec.europa.eu/collection/secure-identity-across-borders-linked-stork/document/stork-20-secure-identity-across-borders-linked-20-stork-20. [Accessed 9 May 2021].

[79 European Commission, “Cross-border digital identification for EU countries: Major step for a trusted Digital Single Market,” [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market. [Accessed 9 May 2021].

[80 J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas and J. Garcia-Blas, “Federated Identity Architecture of the European eID System,” *IEEE Access,* vol. 6, p. 75302–75326, 2018.

[81 Publications Office of the EU , “Connecting Europe Facility,” 2021. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/454df15b-7588-11eb-9ac9-01aa75ed71a1/language-en. [Accessed 9 May 2021].

[82 Connecting Europe Facility, “Documentation eDelivery,” 2021. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITAL/Documentation+eDelivery. [Accessed 9 May 2021].

[83 EU4Digital, “Legislation gap analysis report and recommendations for eTrade policy instruments,” 2020.

[84 X-Road, “X-Road technology Overview,” [Online]. Available: https://x-road.global/x-road-technology-overview. [Accessed 9 May 2021].

[85 X-Road, “X-Road History,” [Online]. Available: https://x-road.global/xroad-history. [Accessed 9 May 2021].

[86 Riigikogu, “Public Information Act,” 2000. [Online]. Available: https://www.riigiteataja.ee/en/eli/518012016001/consolide.

[87 NIIS, “Memorandum of Association of MTÜ Nordic Institute for Interoperability Solutions,” 2017. [Online]. Available: https://static1.squarespace.com/static/59ba41ee64b05fd6531f498d/t/59d1e536914e6b6e0ec0d048/1506928747397/Memorandum+of+Association+of+NIIS+signed_EN.pdf. [Accessed 9 May 2021].

[88 NIIS, “History of NIIS,” [Online]. Available: https://www.niis.org/history. [Accessed 9 May 2021].

[89 X-Road, “CASE STUDY: Iceland joins the Nordic interoperability league with Straumurinn,” [Online]. Available: https://x-road.global/iceland-joins-the-nordic-interoperability-league-with-straumurinn. [Accessed 9 May 2021].

[90 X-Road, “CASE STUDY: Piloting digital prescriptions in Germany through secure data exchange,” [Online]. Available: https://x-road.global/piloting-digital-prescriptions-in-germany-through-secure-data-exchange. [Accessed 9 May 2021].

[91 J. Verhoosel, “Assessment of the maturity of egoverment building blocks for public administrations in the European Union,” in *eChallenges e-2014 Conference,* 2014.

[92 D. Berbecaru and A. Lioy, “n integration of academic attributes in the eIDAS infrastructure to support cross-border services,” in *22nd International Conference on System Theory, Control and Computing (ICSTCC),* 2018.

[93 European Commission, “Coronavirus: Commission proposes a Digital Green Certificate,” 17 March 2021. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1181. [Accessed 9 May 2021].

[94 eHealth Network, “Interoperability of health certificates - Trust framework,” 12 March 2021. [Online]. Available: https://ec.europa.eu/health/sites/default/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf. [Accessed 9 May 2021].

[95 M. Kaevats, *Feedback for the “Interim guidance for developing a Smart Vaccination Certificate”,* 2021.

[96 N. A. Mohamadali and N. F. A. Aziz, “The Technology Factors as Barriers for Sustainable Health Information Systems (HIS) – A Review,” *Procedia Computer Science,* vol. 124, pp. 370-378, 2017.

[97 Publications Office of the European Union, “eHealth Task Force Report – Redesigning health in Europe for 2020,” 2012. [Online]. Available: https://vp2006-2016.president.ee/images/stories/pdf/ehtf-report2012.pdf. [Accessed 9 May 2021].

[98 M. Kimmo, I. Pappel and D. Draheim, “E-Residency as a Nation Branding Case,” in *11th International Conference on Theory and Practice of Electronic Governance (ICEGOV '18),* New York, 2018.

[99 ICAO, “ICAO PKD,” [Online]. Available: https://www.icao.int/Security/FAL/PKD/Pages/default.aspx. [Accessed 9 May 2021].

[10 HL7, “Introduction to HL7 Standards,” [Online]. Available: https://www.hl7.org/implement/standards/index.cfm?ref=nav. [Accessed 9 May 2021].

Appendix 1 – Interview Questions

1. Could you give an overview of recent developments regarding the global trust framework project?
2. What do you consider as the biggest technical barriers?
3. What do you consider as the biggest administrative barriers?
4. What do you consider as the biggest legal barriers?

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

I Katariina Muru

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Global Trust Framework: Pilot for Smart Vaccination Certificate", supervised by Ingrid Pappel.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

10.05.2021

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