TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Ragnar Nurkse Department of Innovation and Governance (RND)

Nata Jokhadze

“Implementation of Interoperability of EU Information Systems in the Justice and Home Affairs Domain. Challenges and Opportunities”

Master’s thesis

Technology Governance and Digital Transformation Programme

Supervisor: Dr. Aleksandrs Cepilovs

Tallinn 2020

I hereby declare that I have compiled the thesis independently

and all works, important standpoints and data by other authors

have been properly referenced and the same paper

has not been previously presented for grading.

The document length is 14982 words from the introduction to the end of conclusion.

Nata Jokhadze …………………………

(signature, date)

Student code: 183812HAGM

Student e-mail address: nata.kentmanni@gmail.com

Supervisor: Dr. Aleksandrs Cepilovs

The paper conforms to requirements in force

……………………………………………

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

………………………………

(name, signature, date)

Table of Contents

Abstract

During the recent years, one of the key things that assisted EU in protection of external borders, mitigating threats and terrorist attacks by increasing internal security was an efficient information management system. Currently there is a need for implementation of interoperability throughout EU-level information systems to exchange and share the information between different agencies and Member States. This thesis focuses on challenges, impacts and opportunities brought by the implementation of interoperability to eu-LISA systems (VIS, SIS II, EURODAC, EES, ETIAS and ECRIS-TCN) and the effect they might have on ordinary citizens, EU institutions and Member States. The results are obtained through literature review of online documents, reports provided by eu-LISA and an interview with Executive Director of eu-LISA – Krum Garkov. Findings identified six key challenges and opportunities that arise during the implementation. Opportunities revolve around new systems being open to the Internet, law enforcement guards being able to access interoperability systems via mobile phones, creation of new information architecture, improvement of information access and the efficiency of services, while providing EU institutions with access to the information from the interoperable systems. Identified challenges included the need of business processes to be redesigned, tight timeline with developments happening in parallel and the need to improve capacity building/training.

Key words: Interoperability, Implementation, New Information Architecture, eu-LISA, Member States

1 Introduction

Currently, interoperability is playing an ever-increasing role in the field of information technology. The concept of “interoperability” will be discussed in more detail below, for now, in the framework of this thesis, interoperability means the ability of systems and components to interact based on the use of information and communication technologies (ICT).

Nowadays people continuously embed new technologies, local and international networks. These implementations allow them to access new communication capabilities as well as boost the speed of the information exchange and solve economic problems that could pose an issue. However, despite the use of technology having undoubted advantages, it raises questions of legal and technological regulation (Singh, 2019). One of the technological problems concerns the interaction of systems. This problem occurs due to the use of technological modelling and standardization by the system manufacturers.

Due to the lack of mutual understanding of technological systems, users have to use the technology of only one manufacturer. At the same time, the mutual openness of systems is an essential characteristic of the information society (Schlagwein, 2017).

In the programme run by the European Commission (EC) to support the implementation of interoperability - ISA[1] (Interoperability Solutions for European public Administrations), interoperability is understood as “the ability of two or more systems or components to exchange information and to use the information that has been exchanged” (IEEE, 1990). Interoperability is one of the main properties of open systems and is achieved through the use of agreed sets of open standards to encourage the use of open source software. One of the basic properties of open systems is interoperability - the ability to interact. Open information systems have a number of features in various aspects of their creation and application. An open system is a system that consists of components that communicate with each other through standard interfaces and emphasizes the systemic aspect of an open information system (Cummings, 2015).

The interaction of open information systems (OIS) is determined by the compatibility of software and hardware components, and therefore, methods and means of data exchange, therefore interoperability reflects the ability of systems to interact without any additional information conversion.

This approach allows you to process, transmit and receive more information in a shorter time which improves system performance, increases the reliability of the system as a whole (due to the use of standard and well-developed technologies in its design), reduces the risk of information loss and distortion or occurrence errors during its transmission (due to the lack of the need for additional information transformations), and also facilitates and accelerates the timely installation of protection against external threats (due to its high level of system compatibility). Thus, properties of interoperability make it possible to increase the efficiency of systems functioning.

In this regard, many of the largest companies face the problem of ensuring interoperability, however, the degree to which their systems comply with this property is different. The appearance on the modern market of information technologies of a wide variety of solutions, characterized by varying degrees of achievement of interoperability increases the need for a single toolkit that allows evaluating the effectiveness of systems in terms of this property.

This thesis will focus specifically on the systems operated by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). Those systems are VIS, SIS II and EURODAC and will be described in more details later on in the text. eu-LISA plays a significant role in implementing and developing interoperability of EU IT systems in the domain of justice and home affairs. It contributes to the success of the EU policies in the area of justice and home affairs and supports the Member States (MS) in their goal to make Europe safer.

The problem of the lack of interoperability in systems has become actively mentioned not only by manufacturers of various systems, but also by the world information community (Olaronke, 2013). Its neglect will lead to difficulties in the application and dissemination, as well as limitation in the choice of various technological systems by users, and therefore, to a limitation competitiveness of information technology (IT) products and enterprises. All of that creates difficulties in information exchange. This especially affects border guards and police where information exchange has to be instantaneous.

In addition, the limitation of the interoperability of systems will negatively affect the organization of e-government in various countries, since the e-government system is built including the use of various technologies. Over the past few years, at the state level and at the level of a number of departments, ensuring interoperability through the use of ICT standards has become an obligatory area of technical ICT policy (Regulation 1025/2012).

The purpose of this thesis is to explain the challenges associated with achieving interoperability within eu-LISA systems and provide better understanding of challenges that come with it.

1.1 Research question

The main question of this thesis focuses on: “What are the issues and opportunities that arise with implementation of interoperability?” The sub questions that help to answer the main question are as follows:

- What challenges in procurement, governance, resource management and operational implementation are linked with interoperability project being implemented by eu-LISA?
- What kind of opportunities will eu-LISA bring with interoperability to ordinary citizens, Member states and EU institutions with optimal usage of the available data?

1.2 Research Methodology – Case Study

Qualitative research is aimed at understanding the essence of the phenomenon (Galliers, 1992). Qualitative methods consider the phenomenon under study as a complex system that cannot be explained by limited reasons. Control over the structure of the research is limited to the preliminary development of a set of questions for data collection and the subsequent study of the patterns between many variables (Stake, 2005). More importantly, qualitative approach was chosen due to the fact that it focuses on textual descriptive data, rather than numerical one (quantitative approach). For the analysis of the implementation of interoperability EU information systems qualitative design was chosen as the best approach. Qualitative research has five main designs: Narrative, Ethnography, Grounded Theory, Phenomenology and Case study. Historical design focuses on description of past events to understand the present ones

(Polkinghorne, 1995). Ethnography is aimed to describe culture's characteristics, like shared patterns and beliefs (Harris, 1968). Grounded theory revolves around discovery and development of a theory (Strauss and Corbin, 1998). Phenomenology is aimed at describing experiences lived by several individuals and what they have in common (Manen, 1990, p. 177). Finally, case study describes in-depth experience of people, community or organizations. Yin defined case study as an empirical study aimed at studying a modern phenomenon in a real context, especially when the boundaries between the phenomenon and the context are blurred (1984). Case studies may include the study of one or several cases (Gerring, 2007, p. 20). In addition, a case can be represented by one or several units of analysis. Based on the definitions of the five qualitative research methods above, it was decided to conduct a case study research as it is better suited for the research questions presented.

There are three types of case studies: Exploratory, explanatory and descriptive (Yin, 2009). Exploratory case studies are flexible and answer questions "what" and "how" to gain deep understanding of a specific phenomenon (Yin, 2014). That kind of research can have a hypothesis, but does not require it to be tested (Darabi, 2007). Explanatory research aims to uncover the issue that has not been studied in depth before and focuses on cause-effect relationships (Yin, 1994). Descriptive approach helps to define the research aspects and portray accurate image of people and events (Robson, 1993). Descriptive case study will not provide the unique insights on the issues like exploratory research would. For that reason the thesis is exploratory case study that focuses on qualitative research.

The role of the researcher grows at the stage of interpretation, which starts at the beginning of data collection, analysis and use of one's subjective understanding of the situation. The meaning of data can be subjective and can be the basis of several interpretations (Klotz, 2008). To minimize wrongful interpretation, the methodology used in the thesis consists of the combination of Primary and Secondary data (Douglas, 2015). Primary data refers to conducting a field study in order to obtain information by the researcher themselves about a particular phenomenon being studied based on the methodology chosen, while secondary data refers to use of available information based on previous studies directly or indirectly affecting the research topic (Mesly, 2015). The advantages and disadvantages of both data analyses methods are listed below (Johansson, 2003 and Vanwynsberghe, 2007):

Primary Data (survey, interview, experiment, etc)		Secondary Data (reports, electronic/printed documentation, etc)	
Advantages	Disadvantages	Advantages	Disadvantages
Focus on a key research issue	The need for additional human resources	Instant data availability	Harder to obtain data relevant to researchers' needs
Better interpretation of the source data	High financial and time costs	Availability of information on the research methodology	Incompleteness of information
Originality, relevance, uniqueness and effective use of information	Insufficient availability of research objects	Low/No cost of obtaining information	Limited data on the data collection process

Figure 1. Comparative analysis of data collection and analysis methods (source: author's own elaboration)

Hence, through combination of these two methods, a more reliable data can be obtained. In this case Primary data refers to the interview with Executive Director of eu-LISA and Secondary data involves document analysis. Document analysis is considered an interpretation of various documents by the researcher and the purpose of this method is to extract and record information from a document, which then will be used to study the research question. (Bowen, 2009). The most common texts for the research are written documents (O'Leary, 2014).

Interview technique will mainly be used, where researcher asks questions and tries to find an answer to that question in the text (O'Leary, 2014). It's important to analyze all the documents available and find information that is related to main questions of the research (Bowen, 2009). Overall document analysis is a process of "evaluating documents in such a way that empirical knowledge is produced and understanding is developed" and it requires a high level of objectivity from a researcher (Triad 3, 2016). Figure below represents the chart of the methodology used in this thesis.

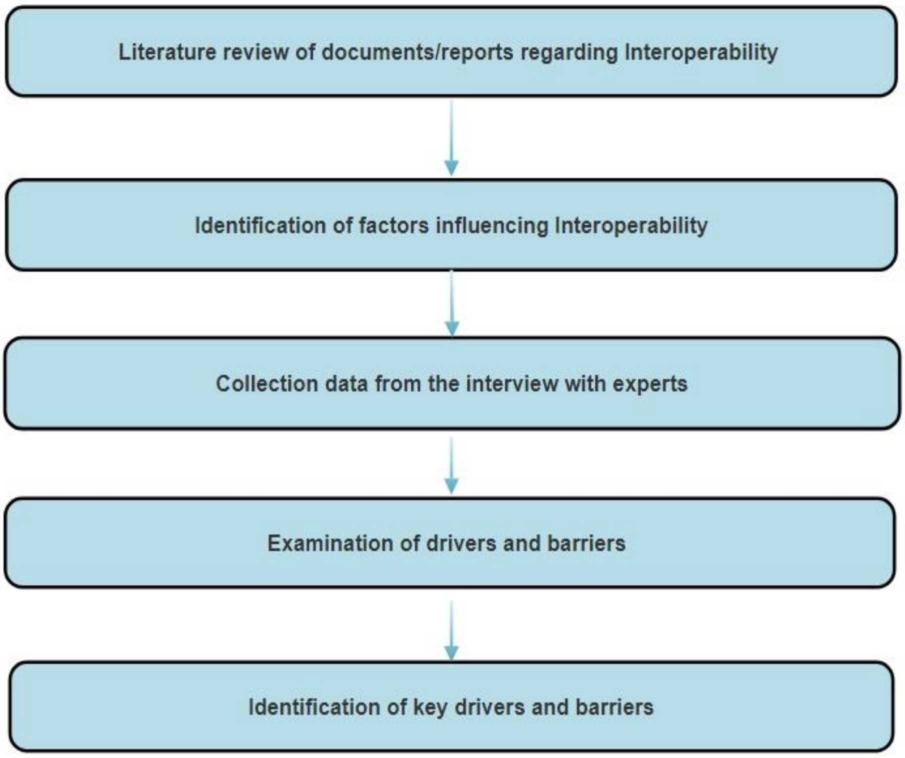
Literature review of documents/reports regarding Interoperability
Identification of factors influencing Interoperability
Collection data from the interview with experts
Examination of drivers and barriers
Identification of key drivers and barriers

Figure 2. Flow chart of the methodology (source: author's own interpretation)

I want to elaborate the reasoning behind selecting both Primary (interview) and Secondary (documentation) data analyses methods. Interview and document analysis were my preferred methods of data collection from the beginning upon going through all possible options. Interview gave me the ability to compare the data from the written reports and documents found online and assess their integrity. It also provided access to the information that couldn't be found online due to the confidentiality. Furthermore, interview allowed me to structure questions in such way, to gain additional information not found online or even in the limited access documents provided by eu-LISA (some of the documents were provided in limited content and some of them were rejected by the Agency – due to sensitivity of those documents). I structured my questions to have direct answer to my main research question.

Another reason why interview was a suitable choice for this case study was due to the fact that some disadvantages shown in Figure 1 weren't present throughout the whole process. The interview didn't require any financial contribution, as it was done electronically (due to COVID-19 pandemic) and I was able to get hold of the Executive Director of the organization who provided reliable data.

Documentation analysis was the main part of my research as it provided the instantaneous access to the information regarding interoperability, eu-LISA together with other relevant EU institutions and research methodology with no additional financial costs involved. However it was harder to obtain data relevant to my specific needs and research questions as at times there was a lack of complete information. That disadvantage was countered by the interview as it allowed me to ask targeted questions.

Based on document analysis and an interview with the Executive Director of eu-LISA, a list of drivers and barriers will be compiled as they influence the implementation of interoperability.

1.3 Theoretical Framework

While researching possible theoretical frameworks for the case study, I came across two most suitable options at the time. One of these options was Enterprise Interoperability Framework. That model was characterized by barrier driven approach which is categorized by three levels of barriers: conceptual, technological and organizational (Chen, 2006). The model deals with barriers, as does my research; however, the barriers presented by this model are of the different type. Chen noted that conceptual barriers referred to syntactic and semantic differences within information exchanged (2006). Technological barriers deal with incompatibility of infrastructures or platforms. And finally organizational barriers refer to delegation of the responsibilities. Additionally, the model includes four enterprise levels of interoperability: interoperability of data, services, processes and business.

All eu-LISA systems are so-called Central Systems, working in collaboration with national systems (i.e VIS, SIS II and EURODAC), therefore eu-LISA systems could be considered as systems working for one organization in cooperation with national systems, which exchange data from national to the central system. It is difficult to state that there are organizational difficulties as each system is different depending on the national state systems. eu-LISA does not have the authority to access the data and at the national level different end users can access different parts of data according to their access rights, but it is not unified in all Member States. In principle, all systems could lack conceptual barriers as syntactic and semantic differences are less notable due to them using the same operational system (Oracle). Despite the fact that systems could be created at different time and could have different technology, they are still part of the central system. It would be difficult to analyze and compare conceptual, technological and organizational barriers of the national systems, especially because the main focus of this research is with regards to eu-LISA central systems.

For that reason, to answer the main research question, a model for understanding interoperability conceptualized by Marc Novakouski (CMU/SEI-2011-TN-014) will be used to achieve goals of successful interoperability. These goals are Process agreement, Meaning Exchange and Data Exchange.

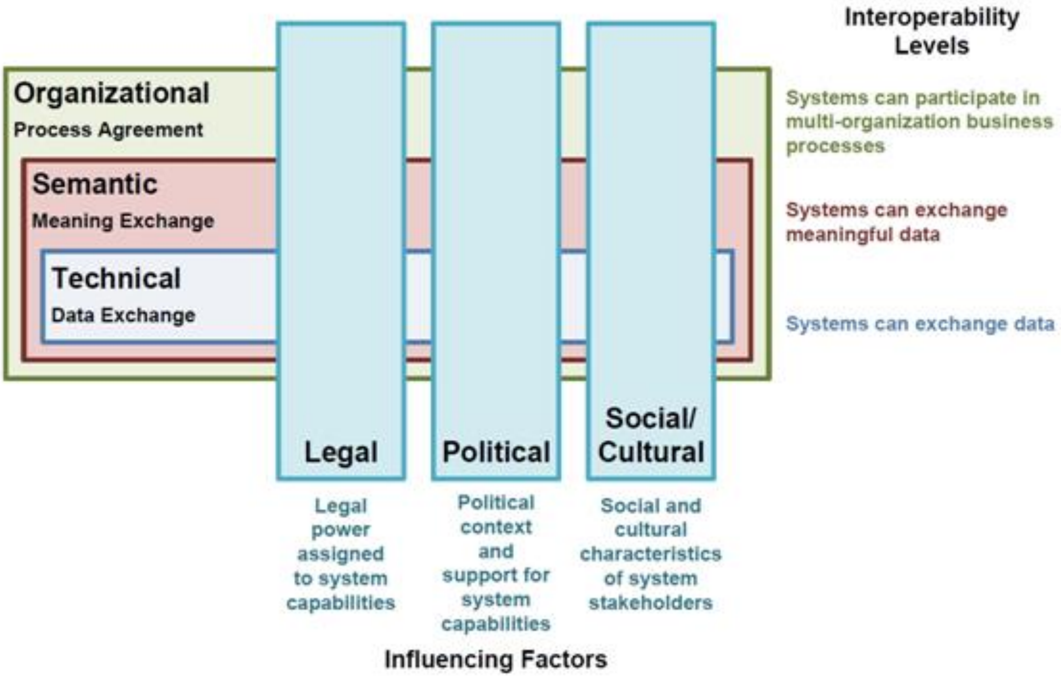
Interoperability Levels
Organizational
Process Agreement
Semantic
Meaning Exchange
Technical
Data Exchange
Systems can participate in multi-organization business processes
Systems can exchange meaningful data
Systems can exchange data
Legal
Political
Social/ Cultural
Legal power assigned to system capabilities
Political context and support for system capabilities
Social and cultural characteristics of system stakeholders
Influencing Factors

Figure 3: Novakouski's Proposed Interoperability Model

Current model also includes Levels which allow interoperability goals to build on each other to achieve more complex goals. These levels of interoperability are: Organizational, Semantic and Technical. Additionally, the model proposed by Novakouski dives deeper to uncover influencing factors such as: Legal, Political and Social/Cultural. These influencing factors have different impacts depending on the organization or any e-Government system. That's why the thesis will focus on applying this model to assess the implementation of interoperability in eu-LISA and find out what challenges and opportunities arise in the process.

2 What is eu-LISA?

EU created decentralised agencies, which are considered as "other bodies" in a Lisbon Treaty language. They are independent agencies covering certain services and policies in accordance with their relevant establishing regulations. One of the areas of the centralized agencies covers Internal Home Affairs, Security and Justice (JHA).

JHA agencies – European Union Agency for Law Enforcement Cooperation (Europol), CEPOL, European Border and Coast Guard Agency (FRONTEX), European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), European Asylum Support Office (EASO) and European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) were created in the European Union to support EU member states in that area. Each agency is unique and has distinct functions. Together, they provide information exchange, preparation and adoption of joint decisions, accumulation of positive experience and assistance in developing a political course in the field of internal affairs. This thesis will focus mainly on eu-LISA as it's currently in the process of implementing interoperability within its large-scale IT systems.

eu-LISA was established in 2011 and began its operations on December 1, 2012 (eu-LISA, n.d.).The Agency carried out operational and management tasks only for these main three systems: SIS (Schengen Information System) II, VIS (Visa Information System) and EURODAC (European Asylum Dactyloscopy database) until the year 2018 (Regulation (EU) No 1077/2011, Article 1(2)). But since then, the Agency became responsible for developing, operating and management of EES (Entry/Exit System), ECRIS-TCN (European Criminal Records Information System on Third Country Nationals) and ETIAS (European Travel Information and Authorization System) in the area of freedom security and justice (Regulation (EU) 2018/1726). One of the main tasks of the Agency is to ensure that these systems support activities 24 hours a day, seven days a week. Other responsibilities include taking the necessary security measures and ensuring the protection and integrity of information in accordance with data protection rules. The headquarters of the Agency is located in Tallinn (Estonia), while the actual operational management is carried out from Strasbourg (France) and St Johan in Pongau (Austria), where back-up systems are located.

The Agency initiated a transformation plan in 2018 to introduce a new organizational structure in line with the current eu-LISA mandate. That program was called eu-LISA 2.0 and was developed to ensure the reorganization process is transparent and includes the staff of eu-LISA (Directive (EU) 2019/1153).

Nowadays, the Agency is adjusting their corporate and operational processes reflecting eu-LISA 2.0. Regardless of how the organization is structured, the main corporate processes as such are still the same (managing budget, human resources, projects, etc). However, there is no a set of processes that fit for any purpose. So there is a need to redesign the processes for the new organizational setup and that’s exactly what eu-LISA has done (K. Garkov, May 2, 2020). The Agency didn’t implement new processes, but rather took the key processes (budget management, human resources, etc.), looked at them across the board and changed them in order to fit the new purpose and the new way of working. From the organizational point of view, they implemented matrix organizational structure, where they have horizontal business lines, which provide a particular set of services to the stakeholders, and vertical lines that contain the organizational structure and organizational entities which provide the resources to enable those services and to deliver them to the stakeholders.

The Agency also implemented a new operating model based on plan-build-run concept, which is common in the IT industry and which has proven to be a right choice for the eu-LISA. Transformation of the Agency is still ongoing and might finish at the end of 2020 or the middle of the 2021. Overall, eu-LISA didn’t introduce new processes, but just redesigned already existing ones in order for them to fit the in the new structure.

2.1 eu-LISA systems and their functionality

As mentioned previously, eu-LISA currently manages three large-scale IT systems (SIS II, VIS and EURODAC) that have to be up and running nonstop and provide constant exchange information in a secure manner. Other three systems (EES, ETIAS and ECRIS) are being developed with go-live scheduled during 2021-2023 depending on the system. Before diving into their interoperability, it’s important to briefly define what each system does and is responsible for.

2.1.1 SIS II

Almost immediately after the signing of the Schengen agreement on June 14, 1985 (SchengenVisaInfo), work began on the formation of a database of all those entering, arriving in the zone states and those who violated the rules of stay or other rules. On April 9, 2013, the second generation Schengen Information System - SIS-II began to operate (Regulation (EC) No 1987/2006). Unlike the first generation SIS, it collects significantly more data about foreigners. Since the amount of data entered and stored in the information system has expanded significantly, a need arose for a special visa section called the Visa Information System (VIS).

2.1.2 VIS

As defined on eu-LISA website (eu-LISA, n.d), Visa Information System processes and exchanges visa information. The VIS consists of a central database, a national interface in each Schengen state and a communication infrastructure between the central database and the national interface. It is connected to the national visa systems of all Schengen Member States through national interfaces, which allows the competent authorities of the Schengen Member States to process data on visa applications, received visas, visa refusals, canceled, revoked or extended visas. VIS continuously processes information collected by consular offices of Schengen states and at the crossing border by the border guards.

2.1.3 EES

Entry/Exit System keeps track of time and location at which third-county nationals enter and exit the territory of Member States while calculating the duration of their stay to prevent illegal immigration. That helps maintaining, securing and managing external borders. According to SchengenVisaInfo, main objectives of EES are improving efficiency of border controls without need of additional guards, combat fraud via electronic checking and detection/prevention of terrorist offences. Overall goal of EES is to ensure a high level of security while managing external borders (Regulation (EU) 2017/2226).

2.1.4 ECRIS-TCN

The purpose of the ECRIS-TCN information database is to facilitate the exchange of information on the registration of criminal offenses in the EU.

The proposed Regulation establishes the creation of a centralized ECRIS-TCN in the eu-LISA agency. The system consists of identification data (alphanumeric data and fingerprint data) of all third-country nationals and stateless persons convicted in member states. A search engine allows Member States to search for content in the internal databases. The data match identifies the EU Member State in which the particular person was convicted. Subsequently, the indicated Member State(s) may be requested to provide full information on the criminal record (OCCRP, 2019).

2.1.5 ETIAS

eu-LISA website states that European Travel Information and Authorization System has one the most important task - to protect Europe from travelers who are a threat. From the moment the system is introduced, any non-citizen of the Schengen member countries will have to obtain permission to enter this system in advance. The main goal of this system is to provide the internal security of every Schengen citizen, as well as people traveling from third countries and making sure people meet entry requirements. It is important for the authorities of the European Union to be sure that tourists from other countries do not pose any danger such as terrorist threat. Those people who do not carry such a threat will automatically get permit, while registering on line to the system

The way ETIAS works: travelers from visa exempt countries are obliged to provide all the information about them before the trip and authorize themselves to enter. Thanks to the system, traveling feels safer.

2.1.6 EURODAC

European Asylum Dactyloscopy database helps to manage asylum applications by collecting biometric fingerprints of people who seek asylum and comparing them with the ones in the database to fight against irregular migration (eu-LISA, n.d). The goal of creating EURODAC is to prevent the possibility of obtaining asylum by the same person in several EU countries at once.

3 Why is there a need for interoperability?

Interoperability is understood as the ability of two or more systems to exchange information and to use the obtained information as a result of the exchange. In order to achieve interoperability data accessibility should be ensured through any other interoperable electronic data systems. All used standards, terms, field values and documents should be understood in the same way and transmitted without loss and distortion between the electronic devices/systems. Interoperability in EU systems should be ensured not only at the technical level through the use of standard communication protocols, but also at higher levels (semantic and organizational). A common vision for harmonizing semantic standards for collecting and accessing metadata must be provided. The relevant eu-LISA systems must have shared biometric matching services, common data repository, single search interface and interconnectivity of the systems.

In 2019, a new legal framework was established between eu-LISA systems in the field of borders and visa (Regulation (EU) 2019/817) and police, migration, asylum and judicial cooperation (Regulation (EU) 2019/818). The objective of these regulations is to create better communications between systems, prevent illegal immigration, create better security and mitigate information gaps.

There are concerns regarding protection of personal data and fundamental rights while making sure all the law enforcement organizations and its members have access to all the necessary information at their disposal (COM (2016) 205 final). While there are systems in place that assist border guards with relevant information, these systems have several shortcomings associated with them that can affect national authorities. The key shortcomings are as follows: sub-optimal functionalities of current information systems, gaps in the EU data management architecture, a dynamic landscape of differently regulated information systems and fragmented data management architecture for border control and protection. The current border control and internal security information systems within the EU cover a broad variety of functionalities, however, the functionalities of the current systems tend to have weak points and drawbacks. Looking at border control procedures applied to various types of travelers it is apparent that there are shortcomings in some of these procedures and in the border control information systems used. Additionally, the efficiency of new law enforcement systems needs to be optimized. And because of that, a need for improvement of these current and new systems is necessary.

Another drawback involves gaps in the EU data management architecture. It is still an issue for border checks of different groups of passengers, like long-term visa holders of the third country nationals. There is also a knowledge discrepancy before border entry as it involves third-country nationals barred from obtaining a visa. Therefore, it should be questioned if these gaps need to be tackled by creating additional information systems where possible.

At EU level, border guards and police officers in particular are faced with a dynamic landscape of differently regulated information systems. Such complexity creates practical difficulties explicitly about which databases in a given situation should be reviewed. In addition, Member States are not interconnected to all currently existing systems. This can be solved by creating a Single Search Interface which allows different nationals to access the systems.

Currently, due to legal, institutional and policy contexts, EU's architecture of data management is fragmented as all of the necessary information is scattered across multiple, mostly not interconnected, systems. Databases are inconsistent and the different authorities have divergent access to data. All of that causes blind spots, especially for law enforcement agencies, as associations between data fragments can be very difficult to identify. Therefore, it is important to work towards integrated solutions to enhance transparency and accessibility for border management and security. Therefore, a move towards the interoperability of current information systems had to be launched.

3.1 How Interoperability will increase efficiency of already existing systems and improve EU's security?

The current border control and internal security information systems within the EU cover a broad variety of functionalities, but in spite of that, system drawbacks still exist and need to be taken into account in order to optimize their functionality (6.4.2016 COM(2016) 205 final).

When border guards check information in the Schengen Information System, they can only search for a name and date of birth. The shortcoming of this system appears to be the fact that border guards are only able to verify a person's identity with fingerprints only after searching and finding their name. This allows potential criminals to use forged documents to avoid SIS identification. To eliminate that drawback of the SIS system, it was proposed and decided by the European Council (2007/533/JHA) to improve fingerprint search by adding Automated Fingerprint Identification System (AFIS).

EC planned to improve VIS functionality by implementing the above mentioned AFIS, creating better quality facial images to make it easier to use biometric matching, allowing collecting younger children's fingerprints between the age of 6 and 12 (SWD(2018) 110 final) and encouraging the use of Interpol's Stolen and Lost Travel Documents (SLTD) database.

EC proposed also to improve and enhance the functionality of EURODAC (COM(2016)197 final). It will track irregular migrants and their movement between Member States as well as identify and re-document irregular migrants which allow them to improve the effectiveness of return and re-admission processes. The legislation would also cover exchanges of information stored in EURODAC with third countries, keeping in mind the data protection safeguards.

4 Interoperability Components

In addition to systems mentioned above, to improve the security of the EU, additional interoperability components need to be implemented - European Search Portal (ESP), Common Identity Reciprocity (CIR), Multiple-Identity Detector (MID), Shared Biometric Matching Service (sBMS) and Central Repository for Reporting and Statistics (CRRS). The components will be used by the same end users who use SIS II, VIS and EURODAC and so on, and not by ordinary citizens. However ETIAS is also accessible for public use (registration for travel to Schengen zone) over the Internet.

4.1 European Search Portal (ESP)

The purpose of ESP being developed is to facilitate quick and efficient access to all eu-LISA systems as well as the EUROPOL and Interpol databases. It acts as a shared search portal that connects all the systems via secure communication channel (Regulation (EU) 2019/817 (Article 6)).

4.2 Common Identity Repository (CIR)

CIR is being created for the purpose of detection and prevention of terrorist offences, supporting MID (see below) and helping correctly identify people that are registered in VIS, EURODAC, EES, ETIAS and ECRIS-TCN (Regulation (EU) 2019/818 (Article 17)). It can collect and store basic biometric and biographical information. If needed, it will be able to correct the identification of third country nationals regardless of the central system. Additionally, eu-LISA together with Member States will implement an interface control document for CIR that is based on Universal Message Format (UMF). CIR won’t be able to alter or modify end-user access rights or deal with new data. Overall, CIR is represented as a component present in all the systems that can store and recover identity data of individuals (such as a birth date).

4.3 Multiple-Identity Detector (MID)

MID is being created solely to support CIR and give access to data stored to central authorities and the Supplementary Information Request at the National Entries (SIRENE) Bureau of the Member State. SIRENE is responsible for any supplementary sharing of information and coordination of activities involving SIS alerts (EC). As it's evident by its name, MID is responsible for detecting if different names link to the same identity and alert the border guards or other law enforcement agent in case of identity fraud (Regulation (EU) 2019/818 (Article 25)).

4.4 Shared Biometric Matching Service (sBMS)

In addition to supporting CIR and MID, sBMS stores biometric templates retrieved from CIR and SIS for querying and comparison of biometric data (Regulation (EU) 2019/818 (Article 12)).

4.5 Central Repository for Reporting and Statistics (CRRS)

CRRS will be responsible for providing analytical reports for policies and for statistical data across all systems anonymously. As rendering data is an anonymous automated process, the access to CRRS will be provided only for the purpose of statistics and reporting (Regulation (EU) 2019/818 (Article 39)). Figure below shows how all of these interoperability components are interconnected (DWP 1.03).

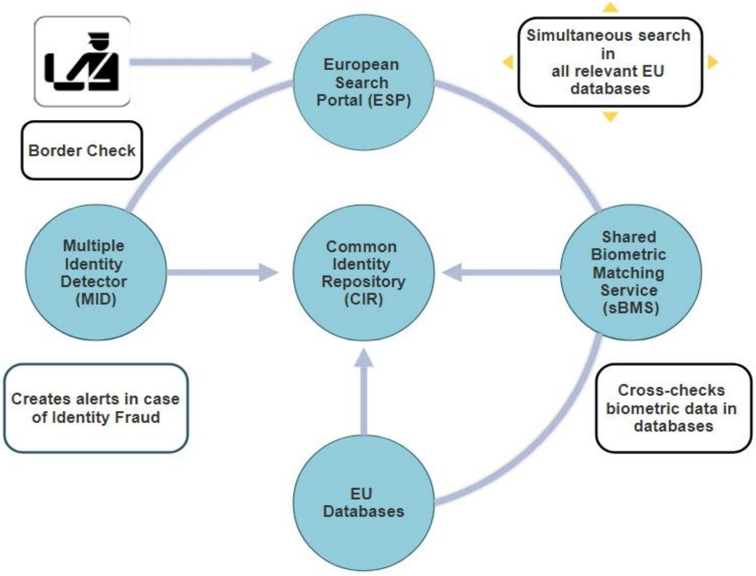
European Search Portal (ESP)
Simultaneous search in all relevant EU databases
Border Check
Multiple Identity Detector (MID)
Common Identity Repository (CIR)
Shared Biometric Matching Service (sBMS)
Creates alerts in case of Identity Fraud
Cross-checks biometric data in databases
EU Databases

Figure 4. Interconnection of Interoperability Components (DWP 1.03)

Besides all the components listed above, eu-LISA was tasked to create an Interoperability Advisory Group (AG) that provides technical expertise and reports to the Programme Management Board (Regulation (EU) 2019/818 (Article 54)).

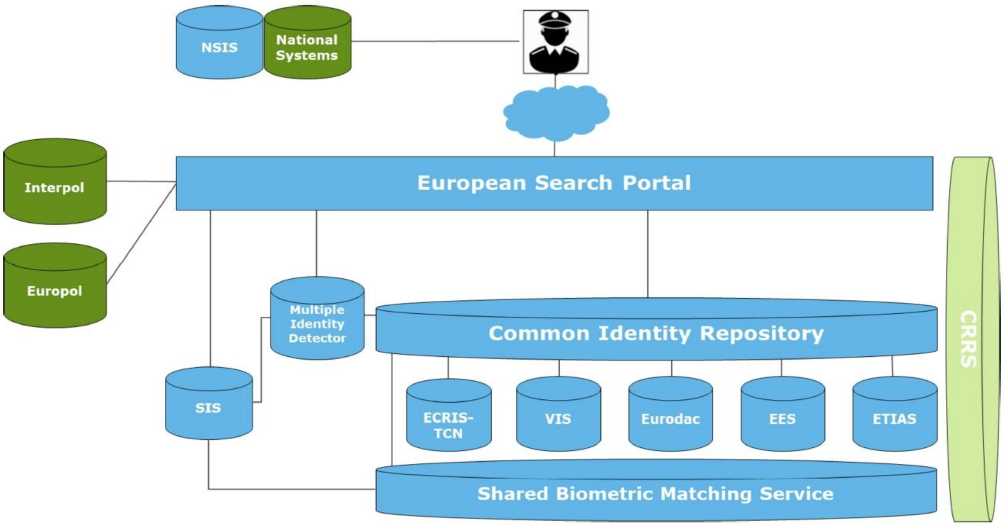

Figure 5. The High-Level Interoperability Landscape (DWP 3.01)

5 Principles and Policies of eu-LISA

5.1 Principles

A principle is a fundamental concept or a rule to be followed in order to ensure that the organizational and IT strategy/aspirations can be achieved. The Principles give guidance to the relevant solutions, while making the claims and decisions more clear and traceable. Principles can contradict one another and priorities must be set for them. "Interoperability Architecture Definition Document" describes the main architecture principles of eu-LISA and lists their prioritization (DWP 1.03). In the case of eu-LISA, data is referred to as an asset that has to be managed properly, maintaining data quality. Main reasoning for that is the fact that Member States entrust their valuable data into the hands of eu-LISA through the use of CBSs (Core Business System) and expect their data to be managed accordingly. Data is the knowledge baseline that will guide future organizational progress, strategies and decision-making.

Business continuity is another principle that has to be considered. Systems become more reliant on each other as they become more ubiquitous and interoperable. The reliability of these systems therefore needs to be assured during their design and continuous usage. Possible hardware failure, natural disasters and corruption of data should not allow disruption or stoppage of system activities as that's eu-LISA's main goal. eu-LISA should have proper business continuity and disaster recovery processes in place to avoid any kind of information loss or data corruption. Dependence on shared system applications involves monitoring and predicting the risks of business interruption or loss of business data beforehand. This can be achieved by constant reviews and testing of critically important systems to make sure no data leakage or loss will ever happen. One solution to that could be storing vital data in different locations.

In order to determine the appropriate security measures to be implemented in the subsequent phases of the project to mitigate the risks and potential adverse effects, newly developed systems or evolution of existing systems must undergo a thorough safety risk analysis from the very beginning of project creation.

Confidentiality, integrity and availability (CIA) are the well-known IT security principles and additional attributes such as authenticity, accountability and non-repudiation may be regarded as subsets of these principles (ISO 27001 and NIST 800 standards). eu-LISA has to follow these principles to abide by legal basis, ensure coverage of security needs, abide by all regulatory considerations and make implementation of interoperability more secure. Additionally, increased business load could come suddenly and the Agency needs to be able to respond to such a request in a timely and efficient manner.

From the beginning, CBS business processes must be structured to conform to data security standards and only process personal data that is required for each particular processing purpose. That includes the quantity of personal data obtained, the degree of their processing, the length of storage and accessibility (derived from the legal basis of the GDPR-General Data Protection Regulation). Specifically, EU regulations, the GDPR and the CBS legal basis require that the privacy of Third Party National be respected and protected within the limits of law.

Furthermore, the data that will be used across multiple systems in application creation must have a common vocabulary in the CBSs to facilitate effective and seamless data sharing. A common vocabulary will make interactions simpler and will allow successful dialogue. The Agency must develop the initial common vocabulary for the CBS, in agreement with its stakeholders. That’s where political factors play a significant role as every agency had to reach a unanimous decision as the definitions selected should be used continuously over the entire lifecycle in all systems.

Every data item has a single authoritative source, which is intended to ensure data integrity within the Member States and eu-LISA. In general, the authoritative source is defined based on the business process that initially collects the data or within the Agency's data asset or business deliverable lifecycle. It’s important to assign the official owner that is responsible for business and operational data as well as its source.

Any collection of safety measures developed for the CBS and its associated processes must be capable of adapting in legal/organizational contexts and evolve to deal with emerging hazards, technical challenges and risks. As new technologies and systems are emerging all the time with additional interoperability requirements, the legal framework is changing. Therefore, the Agency has to be able to adapt new systems, while defining all the risks associated with that whole process.

5.2 Policies

In case of eu-LISA, policies can be divided in three groups: Interoperability Legislation, Core Business System (CBS) Legislation and Security/Privacy Legislations (DWP 1.03).

5.2.1 Interoperability Legislation

The interoperability legislation is composed of two interconnected regulations that outline the future interoperable architecture by introducing five new components of interoperability. Regulations that supplement each other are Regulation (EC) 2017/0351(COD) and Regulation (EC) 2017/0352(COD). These regulations lay the foundations for the future architecture's internal relations, functionalities, and laws. There are major impacts that these interoperability regulations have on eu-LISA's architecture. Documents stated that five new components have to be introduced, developed and maintained (ESP, sBMS, CIR, MID and CRRS). Additionally, it was decided that data (biometric, travel and identity data) will no longer be stored in one place (CBSs) and instead should be stored in CIR. That decision has huge implications on security, data privacy, performance and data protection. Moreover, regulations stated that CBSs won't have their own biometric matching service and instead will switch to sBMS that allows all the information systems to handle the biometric data. The new edition brought out was the use of MID to detect multiple identities across all the systems and not in individual ones. And finally, these regulations strictly define data ownership and retention policies, as well as their storage, quality and protection within interoperability components.

5.2.2 Core Business Systems Legislations

Due to the fact that the interoperability regulation builds on an established and evolving infrastructure, the regulations of the current and foreseen core business structures must also be taken into account in the interoperable architecture.

That's why the following (new and existing) six business systems have to be integrated:

1. VIS (Regulation (EC) 767/2008)

2. SIS II (Regulation (EC) 2018/1860, 2018/1861 and 2018/1862)
3. EURODAC (Regulation (EC) 603/2013)
4. EES (Regulation (EC) 2017/2226)
5. ETIAS (Regulation (EU) 2018/1240 and 2018/1241)
6. ECRIS-TCN (Regulation (EC) 2017/0144(COD))

6 European Interoperability Framework

The priority document for interoperability in the European Union is the European Interoperability Framework (EIF), which shows organizations' willingness to collaborate towards mutually beneficial goals involving sharing of information and expertise between different organizations through the respective business processes assisted by data exchange between their ICT systems. At summit in Seville (2002), representatives of EU Member States adopted the Europe Action Plan 2005 (COM(2002) 263 final), which required Member States to prepare interoperability frameworks that would enable the delivery of pan-European e-government services for citizens and enterprises. The European Interoperability Framework is addressed to e-government project managers in EU member states and European Union institutions.

In 2004, EC published the first version of the European Interoperability Framework, which obliged EU governments to create and support National Interoperability Framework, to ensure interoperability throughout the European Union (EC, 2004).

The European Union faces complicated problems in the field of border and migration management, as well as diverse and overlapping threats to EU internal security. And these exact concerns have brought greater attention to the needs of improving the EU's defense, border and migration information systems. One of the solutions in addressing these needs is the commitment by the EU to take advantage of efficient information sharing and strengthening it among the related EU information systems.

The New EIF (COM(2017) 134 final) focuses on creation of the digital market and aims to improve the quality of European public services. The concept of such interoperability is shown in Fig. 2 below.

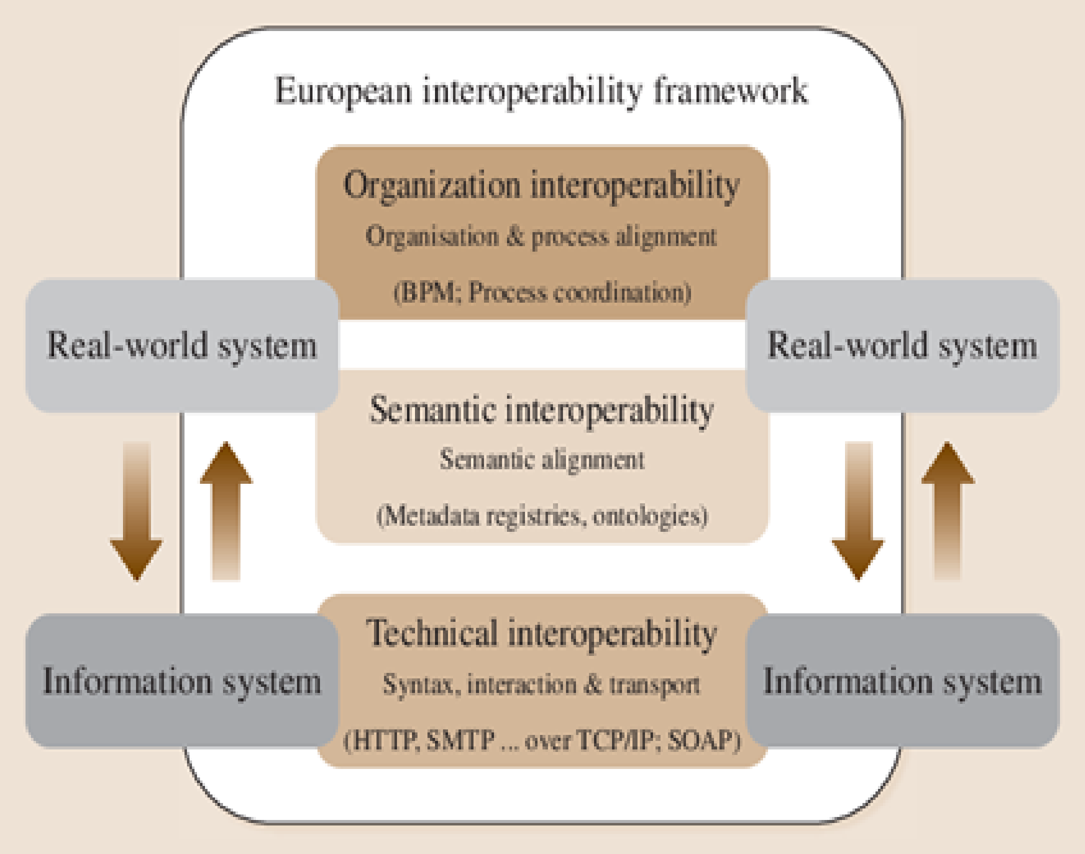
European interoperability framework
Organization interoperability
Organisation & process alignment
(BPM; Process coordination)
Real-world system
Real-world system
Semantic interoperability
Semantic alignment
(Metadata registries, ontologies)
Technical interoperability
Syntax, interaction & transport
(HTTP, SMTP ... over TCP/IP; SOAP)
Information system
Information system

Figure 6: European Interoperability Framework (Vernadat, 2009)

Interoperability model should contain at least three levels: *organizational, semantic and technical*. Data exchange between applied software systems and software platforms that implement information modeling technology (components of information systems) are considered not only from the point of view of technical implementation (the technical level), but also on the semantic and organizational levels.

Technical interoperability includes information exchange, elements of the ICT tele-informatic infrastructure, such as communication lines, computer platforms with operating systems, software in the form of database management systems, a software application for developing the necessary systems and etc. From the interoperability point of view, communication standards at the level of bit transmission in local and global networks, or the transmission of messages between software components are vital (IDABC EIF draft of v.2.0). This level can be divided into other sublevels (Lewis, 2008), but this thesis focuses on the single level.

Semantic level of interoperability should ensure the coordinated functioning of various information systems and their components on the basis of a single, unambiguous interpretation of the value of information obtained as a result of the exchange. It also reflects the need to ensure compatibility of information during data exchange and guarantees the possibility of full access and independent processing of this information by third parties without contacting the owner of the information (Gibbons, 2007).

At the organizational level of interoperability, ways to align business processes at both the internal and external levels should be determined. Thus, business goals are agreed upon and agreements are reached on cooperation and sharing information (Vernadat, 2009).

One of the important changes that came to eu-LISA is with regards to procurement, fundamentally changing it. Previously, the Agency had a "Silo" approach (one single contractor per system) and now it's being replaced by "Transversal Procurement" that allows multiple contractors to work together to mitigate challenges that come with implementation of interoperability.

7 Business and Technical Objectives of Interoperability

There are three business objectives that help to achieve the strategic vision of the EU's architecture of data management and border control through the interoperability implementation (DWP 1.01):

1. EU information systems should be interconnected and Interoperable. In order for border guards and police officers to complete their tasks effectively, it's important to have up to date, relevant and accurate information available to them at all times. Therefore, simultaneous searches across all the systems should be facilitated.

2. Information Systems should be complimentary. Information systems should be interconnected and interoperable, but in no way should they overlap.

3. Modular approach should be pursued. The highest priorities are technological developments, while trying to take principles of "privacy by design" into account by reusing and sharing solutions.

Technical means to obtain the above business objectives are as follows (DWP 1.01)

1. The architecture should give law enforcement fast, systematic and controlled access to information they need, while at the same time getting rid of the complexity of checking every system for the needed information.

2. Detection of multiple identities across different systems should be more efficient to combat identity fraud

3. ESP will aid in correct identification of third-country nationals within the European territory. As it is now, guards have to check different systems to access various records of an individual, making it cumbersome and could possibly lead to oversights during the whole identification process.

4. Law enforcements should be allowed to access non-law enforcement systems to prevent crime and terrorism. It can be done through a new two-step data consultation approach. Officers can check for possible "hit/no hit" (if the match between data entered is found, the officer gets alerted) using CIR, which allows data protection rules to be respected.

5. Strengthen internal and external security and data protection by implementing relevant directives, regulations and security principles (need-to-know and privacy by design) that enforce security controls to specific systems.

8 Novakouski's Proposed Model

In their proposed interoperability model they mention influencing factors. These factors are legal, political (policy), sociocultural and can be applied to any organization regardless of their interoperability levels while having varying impacts (CMU/SEI-2011-TN-014).

All organizations that deal with displaying any sort of information publicly need to address legal issues such as what content can be public, think of political issues such as compliance with existing policies and priorities, and socio-cultural issues such as reaching an audience that might not speak English. All these issues must be addressed and taken into account in order to achieve interoperability. Hence, Novakouski proposed an interoperability model including influencing factors in Figure 2. This model was used as a template to analyse influencing factors of eu-LISA, Europol, Interpol, EASO, FRONTEX, PMB, and Commission/EP/Council.

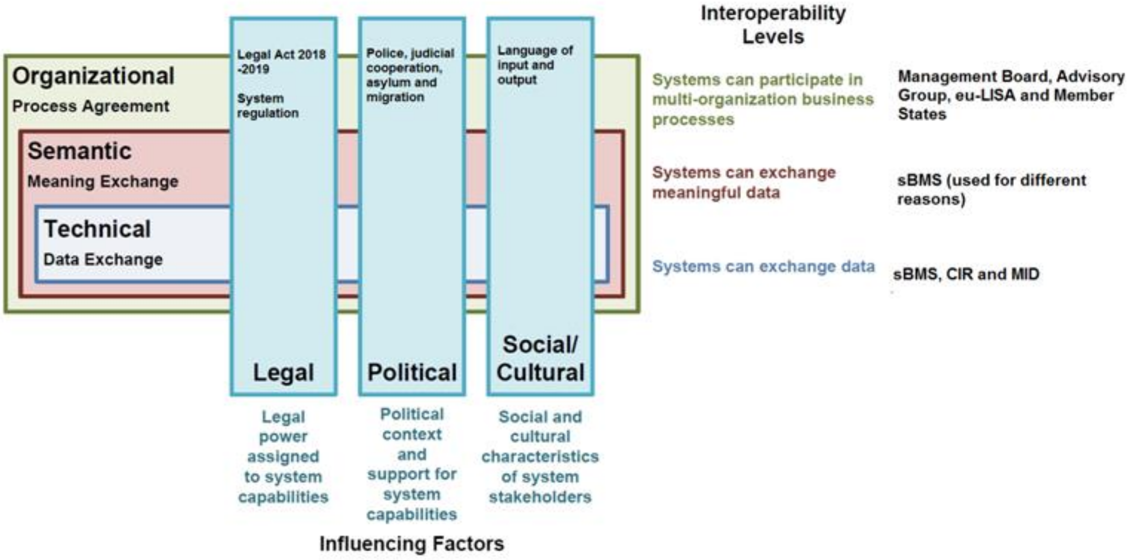
Interoperability Levels
Organizational
Process Agreement
Semantic
Meaning Exchange
Technical
Data Exchange
Legal Act 2018 -2019
System regulation
Police, judicial cooperation, asylum and migration
Language of input and output
Legal
Political
Social/ Cultural
Legal power assigned to system capabilities
Political context and support for system capabilities
Social and cultural characteristics of system stakeholders
Influencing Factors
Systems can participate in multi-organization business processes
Management Board, Advisory Group, eu-LISA and Member States
Systems can exchange meaningful data
sBMS (used for different reasons)
Systems can exchange data
sBMS, CIR and MID

Figure 7. Influencing Factors of eu-LISA

In the case of the framework above, the Organizational level of eu-LISA consists of the eu-LISA Management Board, Program Management Board, Interoperability Advisory Group, Member States, EUROPOL, EASO (European Asylum Support Office), FRONTEX and Eurojust as well as Interpol. Semantic level consists of sBMS and ESP that are used for different reasons across all the systems. Technical level would include all the interoperability components such as sBMS, CIR, MID and CRRS.

8.1 Legal Factors

It’s vital to identify legal issues of public organizations such as eu-LISA to assign responsibility. Organizations must comply with relevant rules, laws and regulations, data protection and so on (European Communities 2008, p.34). eu-LISA is no exception and is responsible for such concerns, especially as it is responsible for developing, maintaining and operating a number of systems. It’s always important for system designers to think through potential failure of any systems and develop appropriate response to such failure. Concerns like that are addressed in the draft 2.0 version of EIF called “legal interoperability” (European Communities 2008, p.34). In his work Novakouski mentioned that dealing with legal issues does not necessarily result in creating a new interoperability goal, but is rather influencing already existing goals (CMU/SEI-2011-TN-014).

The main objectives of the 2017/0351 (COD) and 2017/0352 (COD) legislative measures come from the need to improve the management of Schengen external borders. The following articles of the Treaty on the Functioning of the European Union would form the core legal basis: Article 16(2), Article 74, Article 77(2)(a)(b)(d) and (e) (Regulation (EC)2017/0351-2). Article 16(2) states that the Union shall have the power to take measures in regards to the security of individuals and processing of personal data by the Union organizations, agencies, and by Member States. The Council should take steps to ensure administrative cooperation in the field of freedom and justice between departments of the Member States, as mentioned in article 74. The last article 77(2) talks about Council and European Parliament may take any measure necessary for the step by step establishment of interoperability systems. It’s vital for external borders to be secure and operated effectively. The Member States have agreed to tackle these challenges by sharing information through centralized EU justice and home affairs systems.

Before the use of interoperability components, some necessary conditions are listed in article 76. First of all, necessary training has to be provided on how interoperability components shall be used (Regulation (EU) 2018/1726). Training program should include rules regarding data protection, data security, and obligations listed in article 32(4), 33(4) and 47.

It is vitally important that the components produced conform to the legal basis under which they are introduced and the implementing acts which define them. The individuals responsible for quality assurance should constantly evaluate whether, during the implementation of the project, the design and creation of the systems is compatible with the legal base (DWP 3.02).

One of the legal impacts that affected eu-LISA is regulation (EC) 2017/0351-2 that defines a set of organizational criteria for integrating the components of interoperability. In that regulation, article 54 has the creation of a Programme Management Board.

It's important to define what are the legal concerns related to EU-level information systems and what influence they might have on the implementation of interoperability. In the context of the meetings of the Interoperability Committee and the Expert Group, the Agency assisted EC and Member States in preparation of the relevant legal actions. Together with eu-LISA, the Commission defined the implementing and delegated acts needed for the legal bases to undertake the appropriate procurement actions and to ensure that the Agency will fully comply with the expected implementation timeline. Six acts had to be produced before the end of 2019, five additional ones in the first semester of 2020 and two for the first part of 2021 (PMB Report, 2020-015).

With the new initiatives, there is a huge volume of secondary legislations that are necessary for the Agency to progress bringing benefits and downsides. Whenever there is a need for Member States to be completely aligned (such as in case of data exchange between the Member States), the only way to do it is through regulation. Directives set targets, but leave the mode of implementation more or less open for the Member States to decide. In case of Regulations, however, there are detailed prescriptions that Member States agree upon and that are then implemented across the EU.

The benefit of this approach is that in primary legal acts, there are no more technical details, only political objectives and what needs to be achieved, which was not necessarily the case before (K. Garkov, May 2, 2020). Now, there is more flexibility as eu-LISA works together with the Commission and the Member States to develop the implementing and delegated acts, by addressing relevant issues fit for the purpose. The downside is that the number of delegated and implementing acts requires time to be discussed, agreed upon and adopted. For EES everything is in place, but for ETIAS and interoperability it is a work in progress. The Agency, together with Member States and the Commission, agreed on the schedule prioritizing the implementing acts that have direct effect on eu-LISA's ability to finalize the specifications and do the tenders.

There are potential risks in the legal context associated with the legal environment and requirements, which include the consequences of the potential delay in implementing the consequential amendments to the ETIAS. To possibly mitigate that risk, on the basis of recommendations from EC, eu-LISA will begin the preparation of the Interoperability components tender documentation and will handle changes in the legal acts concerning tenders during implementation (PMB Report 2019). Additionally, the impacts on the timetable and budget for implementation should be closely monitored and change management will be involved, if it is considered appropriate, to ensure alignment of interoperability components with the legal framework at the time of roll-out.

8.2 Stakeholders (Hybrid Factors: Organisational and Political)

eu-LISA, in a way, is a unique agency compared to others EU agencies. The Agency had to start its operations from the day one of its existence, as it had to take over already existing operations and make sure that there were no disruptions to the operations as they are vital for Member States (K. Garkov, May 2, 2020). From the day one of the organization's existence, they proved that what they put in place was efficient and agile enough to deal with everything in a timely manner. It proved that they had confidence and capabilities to do their job correctly and as their operations grew, so did the trust of stakeholders and Member States. Moreover they substantially evolved the existing systems, increasing their value for the stakeholders. Additionally, the Agency became a trusted advisor for the political stakeholders at the EU level (Commission, Parliament and Council) and took part in a number of new developments where providing advice as an expert on capabilities technology to support policy initiatives. And that helped eu-LISA to build a high level of trust towards their ability to do things properly and go beyond what originally was considered as the limit of operations and responsibilities.

Many stakeholders are interested and involved in eu-LISA target architecture. Those stakeholders range from citizens of Europe, going through EU Institutions and Agencies to the Member States. During the project design process, it will be necessary to address the needs of all the stakeholders to deem the project as success. Although every opinion should be considered, there is a high possibility that some may and will have opposing opinions, that’s why it’s vital for the whole project to identify core stakeholders. One of the ways to find out about stakeholder’s needs or opinions is through questionnaires or surveys. They can be sent out to find out their satisfaction with the project or thoughts they have on it, hence allowing to measure stakeholder satisfaction overall (DWP 3.01).

Study done by Deloitte gathered feedback from the survey answers done by stakeholders and showed the need for additional requirements and revealed concerns regarding the project (DWP 1.01). eu-LISA’s concerns revolved around making sure that the quality of the data is up to standard and is secure during processing, transferring and storing. Another concern revolved around architecture being compliant with legal base and being able to adapt to changing requirements in regulations and ensuring adequate system performances while staying in the budget.

EUROPOL and INTERPOL wish their exposed data to be used appropriately. As owners of national systems, Member States want to make sure that the architecture of the project is up to standards and allows necessary functionality and high availability for Member States to continuously operate. Additionally, reduced waiting times and queues at the border checks are needed in order to improve the border crossing process. Co-legislators such as European Parliament and Council are mainly concerned about the security of the EU, quality of the data and privacy legislations. European Data Protection Supervisor that monitors the personal data processing activities of eu-LISA was concerned about proportionality of the measures and ability to easily monitor all activities in the architecture. Main concerns from the European citizens' sides included overall safety of European Union and fair/lawful processing of their personal data with respect to their rights (privacy principles). Third country nationals shared their concerns regarding the speed of processing of border crossings and identifications as well as wishing for border crossing to be reasonably priced and not too inconvenient (K. Garkov, May 2, 2020).

8.3 Political Factors

Success of any interoperability implementation is critically important and relies heavily on political factors. There are four general areas of concern containing barriers regarding interoperability listed in the Gartner report (Malotaux, 2007). Those areas focus on the IT departments, administrations, policy makers and accessibility. What’s interesting is that the list presents only two notes regarding technical issues. But the major common theme remaining is revolving around agency and various department cooperation. In his study, Varney (2006) compiled a list containing six main barriers of interoperability where five of them focus on budgetary issues and coordination. And the draft of EIF 2.0 perceives political factors among the highest levels of interoperability making political support vital for successful interoperability project (European Communities, 2008). In order to assess the level of cooperation between different agencies and Member States it’s necessary to take into account technical, semantic and organizational challenges that affect implementation of interoperability. And political will acts as the driver for addressing the issues that the project may face.

With regards to Stolen and Lost Travel documents Database (SLTD database) mentioned in Interoperability regulation (Regulation (EU) 2019/818) that is run by INTERPOL, in order to have access to this database at the European level, there should be an agreement signed between EU and INTERPOL. According to the Executive Director (ED) of eu-LISA, it is currently happening, but is not in place yet and might not be there at the start of the new interoperability architecture. Additionally, he mentioned that with the time and after they prove their efficiency, there should be further integration of the other systems such as Passenger Name Record (PNR), Application Programming Interface (API) and National systems that are currently not part of interoperability architecture.

What eu-LISA does now is not the end point, but rather one milestone into a big journey for integration of information sources at the European level. It depends on willingness of Member States to exchange data and the information and political courage of all legislators to face the reality that information is the most important asset for internal security and border management. That information should not be hidden behind the closed doors, but rather shared with relevant stakeholders.

8.4 Social/Cultural Factors

Although all three levels of interoperability can be influenced by social and cultural influences, there is another crucial aspect — user adoption. If the implemented information systems do not meet the goal of the government, Member States and especially average citizens, services provided might not be fully adopted.

A survey by TNS Political & Social network in the 28 Member States was carried out to assess the public's opinion regarding their awareness and experiences regarding security. (Special Eurobarometer, 2007). While a vast majority of Europeans in their immediate city and neighbourhood feel safe, they are less persuaded that the EU is a stable place to live in.

Overall, social and cultural factors play, although significant, the minimal role in the implementation of interoperability compared legal and political factors.

9 Drivers and Opportunities

9.1Drivers

Study done by Deloitte identified six core drivers and opportunities for eu-LISA with the help of stakeholders that can be pursued (DWP 1.01). All of the drivers target and shape the architecture of the project in a unique manner and are listed below.

1. Extent to Reuse and Sharing
2. Migration
3. Disaster recovery planning
4. Adoption of Universal Message Format (UMF)
5. Adoption of Service Oriented Architecture (SOA)
6. Integration

9.1.1 Extent to Reuse and Sharing

eu-LISA relies on IT solutions to function with their daily operations and initially developed so-called “silos” as their IT solution as it facilitates greater autonomy while contributing to fragmented IT architecture at the same time. One solution to improve the interoperability of their IT systems as well as to improve the efficiency of operation of IT infrastructure is to share and reuse the IT solutions. In this case “sharing” refers to sharing the same hardware and software components across separate systems while “reuse” refers to the reuse of software. However, this would need the creation and maintenance of a repository of reusable services or hardware that can be shared (DWP 1.01).

9.1.2 Migration

New components of any system rely on existing data and integration of these components does not immediately translate into full operability. Migration in this context refers to only data migration, making it easier to migrate necessary data into the new components. There were two opportunities connected with the data migration and upon thorough research of the Deloitte document, it was recommended to use “Big Bang” migration where all the data is transferred during scheduled downtime of the system.

9.1.3 Disaster Recovery Planning

It is essential for the project’s architecture to have a high availability at all times. And while disasters or other unexpected events occur, sometimes it’s simply impossible to be ready and tackle all of them. Therefore, there is a need for strong disaster recovery planning. One solution to mitigate the effects of the possible disaster is to always have Central Unit (CU) and Back-up Central Units (BCU) active, allowing all websites to be active simultaneously with help of message replication for consistency. It’s also possible to have two physical websites to be active all the time and in case one fails, the other takes over immediately. In the worst case if both of the sites fail, manual activation is required, which takes a significant amount of time to bring both of the sites back to life.

9.1.4 Adoption of Universal Message Format (UMF)

All of the systems have their own formats that they use for information exchange. That's why it's necessary to understand and interpret messages during information exchange between different systems. As every system communicates in their own format, adaptation is needed in order for each system to understand each other. That approach is not ideal and complicates communication and that's exactly why every system should agree on a common message exchange format. That solution also simplifies the design, development and management of systems and that solution became Universal Message Format. UMF is a standard data exchange format that facilitates easy communications between dispersed law enforcement systems and needs to be implemented in interoperable architecture whenever it's possible. All of that allows more messages to be exchanged between eu-LISA systems and law enforcement authorities, especially border guards. In order to implement UMF successfully, a translator for all existing systems can be implemented together with systems adopting UMF standard natively after an internal change.

9.1.5 Adoption of Service Oriented Architecture (SOA)

This Service Oriented Architecture consists of various loosely coupled services with granularity depending on the chosen level of SOA. It provides services to other components through a communication protocol over the network, where the finer the granularity is, the simpler each individual service is. By adopting SOA, eu-LISA facilitates the reuse of services across different functionalities.

9.1.6 Integration

As it stands now, there is an apparent lack of interoperability between the existing systems for security and border management. Systems need to integrate together into complete architecture that allows seamless data transfer instead of working independently in “silos”. One of the opportunities for integration is the integration through the Enterprise Service Bus (ESB). ESB allows to distribute work among connected components of an application and its core principles include Orchestration, Transformation, Transportation, Mediation and Non-functional Consistency. It integrates the existing systems for internal communication, while the use of API led connectivity facilitates the exposure of the external services like ETIAS.

9.2 Opportunities for:

9.2.1 Eu-LISA

In the interview with eu-LISA Executive Director - Krum Garkov, he mentioned that when people speak about interoperability, very often they don't realize that interoperability is not a technical matter. It's possible they got that impression from observing all the new big information systems that are in implementations, but that's not the case. In actuality, interoperability can be considered a political initiative that has to be developed, as a response from the EU, to meet the demand and concerns of the EU citizens for more efficient border management and stronger security. Meaning it's not just a technicality. Another point that was brought up during the interview was that interoperability will bring the range of new capabilities that at the moment are not present or are limited. Those capabilities will change substantially the way border guards, law enforcement and migration officers do their job. Interoperability, in a way, is a big enabler and driver of major transformation of the way border management and internal security are done in Europe.

The biggest opportunity in the overall interoperability project is the creation of the new information architecture for internal security and border management. Alongside with it, the new technological ecosystem is also being built to assist internal security. The most ambitious initiative consists of having a level of standardization of the equipment and solutions to collect all the data and a level of standardization for equipment and solutions needed to access the information that will be managed in the new information architecture. What makes this one of the most ambitious initiatives over the 60 or 70 last years is the fact that many other countries tried to do the same, but not at the same scale and not at the same pace. eu-LISA plans to do everything all together at the same time as well as to deploy an end-to-end approach in 2024, making it not only one of the biggest opportunities, but challenges as well (K. Garkov, May 2, 2020).

9.2.2 Interoperability Systems

The two most important benefits mentioned by Krum Garkov that are part of political agenda are making information access easier and more efficient. Technology deployed in “silos" doesn't really serve a purpose nowadays, as information is the most important asset of the Agency’s data that has to be shared, while dealing with migration management. Another important benefit of interoperability is to link the dots between different “silos”, where information is kept (different information systems) to provide access to this information in a more efficient, transparent and faster way.

The next big benefit comes from deploying a brand new and comprehensive approach for identity management. Krum Garkov brought an example of the 2016 Berlin truck attack on the Christmas market that took the lives of 12 people. After the investigation of German services, it turned out that the attacker had 14 different identities across different European and National systems. For that extract reason a new and comprehensive approach to identity management is an important benefit that interoperability architecture brings in. With interoperability components like sBMS, CIR, MID, ESP and CRRS, that kind of identity theft will not be possible anymore as biometric data remains the same for each individual. That brings a huge positive effect on border management and internal security.

When major new developments will be finished and new information architecture can be deployed, it will be extremely important and crucial for Europe. It will be a focal point for the information exchange related to internal security border management, meaning that Member States and relevant agencies (FRONTEX and EUROPOL) will be very dependent on the information architecture. But that also means it can become a single point of failure if it goes down, bringing lots of negative consequences for the EU. So in that sense, one of the most important objectives while building that information architecture is to make it as resilient as possible in order to minimize the possibility of it being down and mitigate possible negative effects for Europe. It is done through implementation of the so-called Active-Active operations model for the new systems as described earlier.

Situation with existing systems is slightly different as VIS and SIS II have been designed to do best in a “silo” service and the active-active service is not imbedded in them, meaning there needs to be a major architectural change to happen with those systems, alongside with the implementation of the recast of their legal instruments which add a number of new capabilities to those systems. Agency did a comprehensive impact assessment on that, which explored different technical solutions that could be fit for that purpose, selecting the best choice for its needs, which will be implemented gradually over the next two to four years (K. Garkov, May 2, 2020). The EURODAC situation is a bit different as it was the first large-scale system deployed in the area of justice and home affairs. It can be considered old and outdated in all the areas (technically and architecturally), so for the EURODAC, a new system has to be created. EURODAC 2.0 will provide an opportunity to embed the new concept of active-active operations from scratch. Overall, embedding an active-active model of operations into eu-LISA systems will be the biggest change from architectural point of view.

Lastly, Executive Director of eu-LISA mentions the plan for the future to embed a lot of systems into the new interoperability architecture and to have capabilities for mobile phone access. And the reason for that is simply due to the fact that the new interoperability architecture should benefit the practitioners that are on the ground, such as law enforcement officers or the border guard. They don’t have an infrastructure easily available for them on the go, so they need to access the information via mobile devices and mobile networks. That will be essential for the new information architecture and would also require some architectural changes into the systems that already exist. The new information architecture will handle the vast amounts of raw data and information, but the actual value of it comes from its ability to deliver the needed information to the practitioners on the ground at the borders or refugee camps. For that reason mobile phone access and solutions are needed. But that comes with additional risks related to much stronger security levels that need to be put in place.

For the first time, the new systems will be in a way open to the Internet (EES and ETIAS) as big parts of them will interact with travelers and their relevant carriers. So one big change from an architectural point of view will be a much stronger and revised security measures that need to be implemented in order to protect the data that they process from the external attacks.

9.2.3 Member States

For Member States the main opportunity is to improve the efficiency and the effectiveness of the services in the area of border management, increasing their security, especially due to latest terrorist attacks.

Demand for these services increased in terms of their efficiency and the level of protection that Member States provide for the citizens, but under the condition that they are successful at addressing the challenges that are mentioned later in text. On the other hand, the opportunity for the citizens is to get better security and be better protected in terms of better efficiency of governmental services. The broader effects for citizens are to remain the part of one prosperous economical market. Europe has to stay on top of the rest of the world as it is part of the global economy. ED mentioned that in 2017 people that came from other countries to European Union for various reasons contributed almost 300 Billion Euros to the European Gross Domestic Product (GDP). The direct benefit for European citizens besides the stronger security will be that interoperability and the way it will facilitate more efficient border management and better security will also support the economic growth.

9.2.4 FRONTEX and EUROPOL

As of now, neither FRONTEX nor EUROPOL have access to the information regarding internal security border management that is important for them in order to do their job efficiently. Currently there is a process of expansion of FRONTEX, where they are recruiting standing corps of border guards who will be deployed at the external borders of the Union and will support Member States in protection of those external borders (FRONTEX, 2019). However, as stated by Krum Grakov during the interview, if they are just deployed there without having access to proper information, their work will be inefficient. And for that reason, being part of that new information architecture will benefit FRONTEX and EUROPOL tremendously from an operational point of view by having access to the information brought by interoperability systems in order to improve their workflow. In the old days, a border consisted of a fence and the number of the border guards behind the fence to guard it. Today, however, the actual borders are digital and countries are protected not by fences or a number of border guards, but by the amount of information these countries or agencies collect and use in order to make proper risk assessments and to decide where and how to focus their efforts and resources.

10 Barriers and Challenges

10.1 Barriers

One of the main barriers is in regards to security and privacy policies as the whole project must be in alignment with up to date EC's decisions of ICT security. The example can be implementing rules (2017/8841 and 2018/559) and Commissions' decision (2017/46). Additionally, proposals for interoperability regulations dictate a specific timeline by which the new systems should be operational, while supporting interoperability requirements (2017/0351 and 2017/0352). These revision proposals are still going through the legislative procedures of Council, EC and European Parliament.

Other major concerns include the fact that eu-LISA has to solely rely on external contractors to develop and obtain software solutions while making sure that this software meets all the requirements necessary and doesn't exceed the budget. While the whole implementation occurs, currently functioning systems should not be impacted in any way. If they are, there should be a mitigation plan in place supported by a reasonable budget, as financial resources of the Agency are not limitless. As the Interoperability Regulation is largely based on the other information systems' legal bases, changes to those legal bases can have a major impact on the design and implementation of the interoperability. Another worry comes from fear of the main system collapsing due to availability issues at network level affecting the central component.

10.2 Challenges for:

10.2.1 Eu-LISA

From the Agency point of view, interoperability and new information architecture is transversal (horizontal) as it connects the dots between the “silos" that exists and for that reason in order to be able to manage this new architecture properly, its internal structure and capabilities have to be aligned with new demand coming from the stakeholders. For that reason the Agency implemented so called eu-LISA 2.0. Historically, the Agency started as a classic IT organization, meaning it was built around several big “silos” representing the existing systems and easy “silo” had its own stack of services and supplies going from A to Z (K. Garkov, May 2, 2020). But that was inefficient and was not fit for the purpose, as the new mandate required the Agency to be more transversal than it was before. For that reason, already in 2018, eu-LISA started major organizational transformation in order to ensure that organization is fit for its new purpose. That transformation had several important elements like the new organizational structure of the agency, the new operating model and the cultural shift. It’s not enough to implement just the organizational structure. The Agency has to make its work by having people learning in the new organizational context, which is not easy as most spent their entire working career in a “silo” based organization. So the cultural shift is very important for that transformation.

There are several big challenges that go beyond the technicalities, when interoperability is mentioned. The first major challenge mentioned during the interview alongside technical development was the fact that a lot of attention needs to be paid to redesign of the business processes. Even with having the most perfect technology, if old fashioned business processes are integrated, the added value will not be as expected. So redesigning business processes and changing the way border guards and law enforcement officers’ work is one of the biggest challenges of interoperability.

Another challenge, mentioned by ED, in the same line is the capacity building. It is not enough to deploy new technology, people need to make sure that those who will have access to the capabilities provided by the new technology will understand them and will be able to utilize them to the maximum capacity in the most efficient way. That makes capacity building and training for the Member States the second biggest challenge that eu-LISA faces, as the number of people that will have access to those new capabilities and functionalities across the whole EU border is extremely high. According to Krum Garkov, there are more than 800,000 SIS II users, law enforcement officers, border guards, migration officers and all of them need to know how to use the new systems and utilize their capabilities.

The third challenge is related to the industry. The timeline for the implementation of interoperability is tight, as everything has to be completed by the beginning of 2024. That means there is a high demand for various equipment and technology to be deployed rapidly in the Member States and at the central European level. The challenge consists of whether industry is prepared for that huge new demand, especially now in the context of COVID-19 crisis which took a toll on the global economy. Industry will have to shift to provide end-to-end integrated solutions. When such huge initiatives like interoperability implementations are mentioned, the measure of success is not outstanding. The level of success depends on the level of trust that government and politicians as a whole can build with the citizens by addressing concerns of those citizens. It's important to provide necessary safeguards for privacy and provide the reassurance that the data collected (interoperability collects vast amounts of data) is used for legitimate purposes rather than global surveillance. Fundamental rights and privacy are extremely important for these kinds of initiatives and if not addressed properly, the results and usefulness will be challenged/questioned by citizens, no matter how advanced and efficient the technology is.

10.2.2 Member States

Member States also have to change the way they are organized in order to benefit from the new interoperability architecture. That includes working in the more translucent way, to collaborate/cooperate much more horizontally across the government structures, to redesign the business processes and to invest into the capacity building (K. Garkov, May 2, 2020). Those changes are vital for the overall success of the initiative. Even though there are a lot of technologies behind it, it is not a technical initiative, but rather a huge transformation program for internal security and border management in Europe, driven and enabled by technology.

Overall, the biggest challenge for them is to have the ability to follow the ambitious and tight implementation schedule (K. Garkov, May 2, 2020). There is a need for a lot of coordination on the national level for the work to be done, as it is very complex (redesigning business processes, capacity building, procurement procedures). In Member States, different agencies are responsible for building blocks of interoperability. EES is normally under the jurisdiction of the Ministry of Interior, while ETIAS most likely will be under the jurisdiction of the Ministry of Foreign Affairs, so there is lots of coordination between these two ministries and many other national agencies. National political environment may influence the ability of the Member States to deliver on time, as currently most are concerned with COVID-19 crisis and its effect on the economy.

10.2.3 eu-LISA Systems

Another huge challenge for eu-LISA is the fact that all of the developments are happening in parallel. They are not consequential and need to start operating together, as they all represent major building blocks of the information architecture and are interdependent (K. Garkov, May 2, 2020). Currently, eu-LISA is very advanced with the implementation of EES, but ETIAS depends a lot on the progress of implementation of EES, whereas interoperability architecture depends on progress of implementation of EES and ETIAS together. They are all interconnected and depend on one another and on top of that eu-LISA also has to focus on the evolution of already existing systems (VIS, SIS II, and EURODAC) in order to fit into the new architecture. The biggest challenge for the Agency in that sense is to sustain its operational and corporate capability, making sure that existing systems are up and running for Member States and to progress in a timely manner the implementation of the initiatives.

Consequential amendments on ETIAS regulation add relevance into requirements for ETIAS and EES, but those amendments together with revision on VIS regulation are currently on hold in the Parliament due to the crisis (K. Garkov, May 2, 2020). All of that had an effect on the agency and is considered a major external risk, with added possible shifts of political priorities due to COVID-19 crisis. Before the crisis, the Commission submitted its proposal for the Multiannual Financial Framework (MFF), which provides a long term budget for the EU for the next seven years (2021-2027) with certain priorities. However, most likely there will be a refocusing of priorities to deal with the aftermath and consequences of the crisis. There is a level of uncertainty whether or not current actions of eu-LISA will remain as part of the political priorities.

10.2.4 Procurement

The major challenge is the scale of the procurement, as the portfolio of projects is at a total value of more than a billion of Euros. As part of eu-LISA 2.0, the contractual architecture also had to be redesigned and moved away from "silo" to translucent contracts. It can be destructive for the market as companies have to find the way to address these demands by creating alliances that didn't exist before. And to manage all that lots of resources have to be allocated to ensure that eu-LISA is compliant with all the regulatory requirements. There are also risks involved and one of them is reputational. If tenders are not managed properly, the reputation of the Agency is bound to suffer. Beyond that, there is also a substantial financial risk involved. If something goes wrong, there will be damage done to the European budget, possibly wasting lots of public money. And to ensure that likelihood of something like that occurring is low, eu-LISA implemented strong and robust internal controls (K. Garkov, May 2, 2020).

11 Analysis

By outlining influencing factors affecting eu-LISA, EU information systems, EU Institutions and Member States, the Novakouski's Interoperability Model allowed me dive deeper into understanding the issues brought out by the implementation of interoperability. Legal, Political and Social factors revealed a number of challenges as well as opportunities faced not only by eu-LISA, but also institutions mentioned above. My research uncovered six main challenges and opportunities that come with interoperability implementation.

Key Drivers/Opportunities	Key Barriers/Challenges
1. Access to interoperability systems through mobile phone	1. All developments are happening in parallel at the same time and are co-dependent

2. Creation on new information architecture for internal security and border management	2. eu-LISA business processes have to be redesigned
3. Improving the efficiency and the effectiveness of the services in the area of border management in Member States	3. Capacity building and training
4. Making information access easier and more efficient	4. Limited resources and dependency from political developments
5. New systems being open to the Internet (EES and ETIAS)	5. Member States will have to redesign their business processes adapt translucent way of working
6. Providing other agencies like FRONTEX and EUROPOL with access to the information from the interoperability systems	6. Tight timeline for interoperability implementation

Figure 8. Key Challenges and Opportunities (source: author's own interpretation)

I'll focus on key barriers and challenges first:

1. All developments are happening in parallel at the same time and are co-dependent. The developments regarding new systems (EES, ETIAS and ECRIS-TCN) are happening in parallel. VIS, SIS II and EURODAC are functioning, but VIS is supposed to be upgraded and there possible delay in the recast in EURODAC. If one

of these systems will have a delay due to, for example, some difficulties with the contractors, the full interoperability will not have a full functionality. So the full functionality of the interoperability systems will be delayed. Overall interoperability will be eventually done, so the issue is only with optimal and full functionality. There is the development of interoperability itself and if that is delayed, the whole functionality will not be in place. It's of paramount importance to have no delay in the interoperability parts and if there is delay in other elements like EES, ETIAS and ECRIS-TCN, it means that optimal utilization of the system will be affected.

2. Business processes have to be redesigned. Implementation of the new operating model might be delayed and there might be delays in a processing of the requests for change as well as delay of the full implementation of budget and cause the delay in overall project management related to interoperability. Redesigning will possibly have some inefficiencies, so it should be the main focus of the eu-LISA staff and management to finalize the redesign of the business processes as soon as possible as it will have effect on all the elements.

3. Capacity building and training. Capacity building is not urgent at the moment for the training as the training will be done later on when the systems are already in place. Any delay in the preparations of the training will not have a significant effect as all the elements will be ready in the couple of years. It is important for the long term implementation, but a small delay in the capacity building and optimization is not a major issue, especially because there is still time to prepare outsourcing of the training if needed.
4. Limited resources and dependency from political developments. If the renewal of amendment on interoperability will not create contradictions to existing features, they can be added later on. They might have no influence on the delay, but instead provide additional benefits in the future. However, if the amendment will result in the substantial changes in the current information architecture, that could result in the delay of the current implementation. In the worst case scenario it could result into more budgetary needs and the delay in overall implementation and the best scenario, current implementation goes as planned with additional benefits added later on. If the amendment will require substantial changes in the current legislation and changes in the technical design of interoperability, the whole process has to be put on hold.

5. Member States will have to redesign their business processes adapt translucent way of working. It’s equally as important for the Member States to redesign their business processes as it is for eu-LISA. However, Member States are end users, so they have more time until the systems are operational or at least in the testing phase, making it more vital for eu-LISA to redesign their business processes.

6. Tight timeline for interoperability implementation. In the scenario where all Member States are ready, but the central system is not, one of the ways eu-LISA can speed of the process is by putting money into additional resources, such as extra employees. If Member States are also faced with a delay, the only drawback is being late, with no additional financial implications. Any delay, be it in the procurement or recruitment of staff, might impact reputation of eu-LISA. Not having systems done on time will be a small drawback as already existing systems will still continue to work. However, the reputation of eu-LISA may be damaged.

One of the key opportunities includes access to interoperability systems through mobile phone. However, there is a risk in adjustment of legal basis in some Member States is necessary in order to allow having access to systems on the mobile devices. It is a huge opportunity for border guards in trains, on the boats and car crossing points, where law enforcement officers have to physically go face to face with people instead of waiting for them to come. Political willingness and approval of legal basis must be done on time, but upon its completion, it should dramatically improve usability of the systems.

Creation on new information architecture for internal security and border management will provide full scalability of the systems and the long term end economy. From the economical point of view, on the long term development of information architecture is the most important part.

Improving the efficiency and the effectiveness of the services in the area of border management in Member States will allow people to wait shorter time at the checkpoints. It also is liked to opportunity of adding mobile phones, making information access easier and more efficient for better time management at cross borders.

New systems being open to the Internet (EES and ETIAS) is an opportunity but also a big risk. Certain elements of ETIAS should be open over the Internet, so the system must be bulletproof in a way to prevent any sort of hacking. It will be easier for end users to enter and obtain required documents, but at the same time it’s a high risk eu-LISA must address and ideally mitigate.

Providing other agencies like FRONTEX and EUROPOL with access to the information from the interoperability systems will have additional opportunities. eu-LISA facilitates a work of other agencies, not only the citizens. FRONTEX will provide border guards to the Member States if requested and EUROPOL will provide information to eu-LISA systems regarding criminal activities, while having access to their systems.

12 Conclusion

Throughout recent years, there has been a significant change in the fields of border control, internal security and migration management, shifting from the physical to the virtual environment. The heterogeneity of EU information systems currently in place makes data access unnecessarily complicated. It can lead to blind spots for law enforcement agencies, as links between data fragments can be very difficult to identify. This fragmentation is tackled through the interoperability of the different information systems at EU level. This ensures that systems should be able to complement one another, so that when they need it, the appropriate people have access to the information they need.

The Commission is completing this work by introducing new instruments for developing the EU information systems and ensuring cohesion between them. Interoperability between systems will help to tackle irregular migration, correct identification of persons, combat identity fraud, validate travel documents and ultimately contribute to a higher level of security within the Union's area of freedom, security and justice.

It’s the main focus of the EU Commission is to mitigate the threat to safety and security of citizens. Reducing the number of tourists is not favorable as they are linked with economic growth. The fact that systems like VIS, SIS II and EURODAC were created in different times with different technologies, created a need for interoperability to unify all of these systems and reorganize them for the optimal use. It will be done for the benefits not only of eu-LISA, but also for citizens, EU institutions, other Agencies and Member States.

Nevertheless, implementation of interoperability brings not only opportunities, but challenges as well. That's why this thesis explored the challenges in procurement, governance, resource management and operational implementation, while also focusing on what kind of opportunities the implementation will bring to ordinary citizens, Member states and EU institutions. Throughout the independent research, online documents and reports provided by eu-LISA I was able to identify key challenges and opportunities of the interoperability implementation listed below in Alphabetical order.

Key Drivers/Opportunities	Key Barriers/Challenges
7. Access to interoperability systems through mobile phone	7. All developments are happening in parallel at the same time and are co-dependent
8. Creation on new information architecture for internal security and border management	8. Business processes have to be redesigned
9. Improving the efficiency and the effectiveness of the services in the area of border management in Member States	9. Capacity building and training
10. Making information access easier and more efficient	10. Limited resources and dependency from political developments
11. New systems being open to the Internet (EES and ETIAS)	11. Member States will have to redesign their business processes adapt translucent way of working

12. Providing other agencies like FRONTEX and EUROPOL with access to the information from the interoperability systems	12. Tight timeline for interoperability implementation

The project is extremely important from the political point of view, risky and costly from the financial point of view and full of challenges as it is the most substantial project of the last 60 or 70 years, as stated by eu-LISA Executive Director. However, despite all of that, I am convinced that implementation of interoperability will be successful and will bring all the necessary benefits for the eu-LISA, EU institutions and Member States.

13 References

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. Qualitative Research Journal, vol. 9, no. 2, pp. 27-40.

Chen, D. (2006). Enterprise Interoperability Framework. EMOI-INTEROP 2006 (Co-located with CAiSE 2006): Luxembourg

Commission Decision (EU, Euratom) 2018/559 of 6 April 2018 laying down implementing rules for Article 6 of Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission.

Commission Implementing Decision (EU) 2019/1269 of 26 July 2019 amending Implementing Decision 2014/287/EU setting out criteria for establishing and evaluating European Reference Networks and their Members and for facilitating the exchange of information and expertise on establishing and evaluating such Networks.

Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation Of The European Parliament And Of The Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement. SWD/2018/110 final - 2018/0104 (COD)

Communication From The Commission To The European Parliament And The Council Towards A Reform Of The Common European Asylum System And Enhancing Legal Avenues To Europe. COM/2016/0197 final

Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. European Interoperability Framework – Implementation Strategy. COM/2017/0134 final

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

Cummings, T. (2015). Organization Development and Change. Cengage Learning, Vol.10 , 13-21.

Darabi, F. (2018). Developing General Analytical Inductive Qualitative Research Strategy to Explore Small Enterprise Growth in Turbulent Economies. Conference: 17th European Conference on Research Methodology for Business and Management StudiesAt: Universita' Roma TRE, Rome, Italy

Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties

Deloitte (2018). Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA (DWP1.01)

Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Douglas, B. (2015). The Theory and Practice of Development Education: A Pedagogy for Global Social Justice. Routledge; 1 edition.

Douglas, M. (2015). "Sources of data". Retrieved on 26th April, 2020 from http://www.onlineetymologydictionary/data

eu-LISA (2019). Amendments by Interoperability Regulations (DWP1.01)

eu-LISA (2019). Interoperability Architecture Definition Document (DWP1.03)

eu-LISA (2019). Interoperability Architecture Requirements Specification (DWP1.02)

eu-LISA (2019). Interoperability Requirements Impact Assessment (DWP3.01)

eu-LISA (2019). PMB Report

eu-LISA (2020). PMB Report

eu-LISA (2020).Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA, Impact Assessment and Migration and Integration Plan

eu-LISA (n.d.). VIS, SIS II, EURODAC

European Commission (2002). eEurope 2005: An information society for all

European Commission (2004). European Interoperability Framework

European Commission (2007). Eurobarometer Special Surveys

European Commission (2014). European Interoperability Framework (EIF) for European public services

European Commission (2016). Stronger and Smarter Information Systems for Borders and Security

European Commission (2017). European Interoperability Framework – Implementation Strategy

European Commission (2018). The implementation of the Action Plan to strengthen the EU response to travel document fraud

European Commission (2019). About ISA².

European Commission (n.d). SIRENE Cooperation

European Commission (n.d). SIS II - Second generation Schengen Information System

European Parliament (2019). Interoperability between EU information systems (borders and visa)

European Parliament (2019). Interoperability between EU information systems (police and judicial cooperation, asylum and migration)

European Parliament (2020). The European Council and the 2021-27 Multiannual Financial

Framework

Frontex (2019). The Expansion of Frontex: Symbolic Measures and Long-term Changes in EU Border Management

Galliers, R. (1992). Choosing Information Systems Approaches.

Garkov, K. (2020). Independent Interview.

Gerring, J. (2007). An Experimental Template for Case Study Research. Midwest Political Science Association.

Gibbons, F. (2007). Better Dispute Resolution: A review of employment dispute resolution in Great Britain.

Harris, M. (1968). The Rise of Anthropological Theory: A History of Theories of Culture. The University of Chicago Press.

IDABC (2004). European Interoperability Framework for Pan-european eGovernment Services

IDABC (2005). European Interoperability Framework v 1.0.

IEEE (1990). Interoperability, Composability, and Their Implications for Distributed Simulation: Towards Mathematical Foundations of Simulation Interoperability

Johansson, R., (2003). Case Study Methodology, Volume 18, No. 1, Art. 19.

Lewis, A. (2008). “Why Standards Are Not Enough To Guarantee End-to-End Interoperability”. Seventh International Conference on Composition-Based Software Systems (ICCBSS).

Malotaux, N. (2007). Controlling Project Risk by Design. Vol17, Issue1. San Diego, CA, 1153-1167.

Manen, M. (1990). Researching lived experience: Human science for an action sensitive pedagogy. State University of New York Press; 2nd ed. Edition.

Mesly, O. (2015). Creating models in psychological research. International Journal of Traffic and Transportation Psychology Vol. 3, Issue 1.

MITA (2009). National ICT interoperability framework.

Novakouski, M. (2012). Interoperability in the e-Government Context. 7-12

O’Leary, M. (2014). Classroom Observation - A guide to the effective observation of teaching and learning. Routledge, 1st Edition.

OCCRP (2019). EU Green Lights Database of Convicted Non-EU Citizens.

Office for Official Publications of the European Communities (2004). European Interoperability Framework For Pan-European eGovernment Services.

Olaronke, I. (2013). Interoperability in Healthcare: Benefits, Challenges and Resolutions. International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 3 No. 1

Polkinghorne, D. (1995). Narrative configuration in qualitative analysis. International Journal of Qualitative Studies in Education 8 (1): 5-23.

Proposal for a Directive Of The European Parliament And Of The Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA

Proposal for a Regulation Of The European Parliament And Of The Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and

amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)

Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance

Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

Robson, C. (1993). Real World Research. A Resource for Social Scientists and Practitioner Researchers. Blackwell Publishers Inc., Oxford.

SchengenVisaInfo (n.d.). What is Schengen?

Schlagwein, D. (2017). “Openness” with and without Information Technology: a framework and a brief history. Volume 32, Issue 4, pp 297–305

Singh, J. (2019). Regulating Recommending: Motivations, Considerations, and Principles. Forthcoming, European Journal of Law and Technology.

Stake, R. (2005). Qualitative case studies. The Sage handbook of qualitative research (p. 443–466). Sage Publications Ltd.

Strauss, A and Corbin, J. (1998). Basics of qualitative research: Techniques and procedures for developing grounded theory, 2nd ed. Sage Publications, Inc.

Techopedia Inc. (2020). Interoperability.

Triad 3 (2016). An Introduction to Document Analysis.

Vanwynsberghe, R., (2007). Redefining Case Study. International Journal of Qualitative Methods.

Varney, D. (2006). Service transformation: A better service for citizens and businesses, a better deal for the taxpayer. Published with the permission of HM Treasury on behalf of the Controller of Her Majesty's Stationery Office.

Vernadat, F. (2009). Technical, Semantic and Organizational Issues of Enterprise Interoperability and Networking. IFAC Proceedings, Vol. 42, Issue 4, 728-733

Yin, R (2014). Case Study Research Design and Methods (5th ed.). Journal: CJPE; Volume 30; Issue: 1.

Yin, R. (1984). Case Study Research: Design and Methods. Sage Publications, Beverly Hills, California.

Yin, R. (1994). Case Study Research: design and methods. Second Edition. International Educational and Professional Publisher Thousand Oaks.

Yin, R. (2009). Case study research: Design and methods (4th Ed.). Thousand Oaks, CA: Sage.

Non-exclusive licence

A non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I ________Nata Jokhadze__________ (*author's name*)

1. Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

____"Implementation of Interoperability of EU Information Systems in the Justice and Home Affairs Domain. Challenges and Opportunities." ___,

(*title of the graduation thesis*)

supervised by_______Dr. Aleksandrs Cepilovs__________,

(*name of the supervisor*)

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author will also retain the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*