TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technology

Maris Järvsoo, 153210IVGM

IMPLEMENTATION OF INFORMATION SECURITY IN EU INFORMATION SYSTEMS WITHOUT UNIFIED SECURITY STANDARD

Master's thesis

Supervisor: Alexander Horst
Norta
PhD

Co-Supervisor: Elin Iloste

MBA

Tallinn 2017

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Maris Järvsoo, 153210IVGM

EUROOPA LIIDU INFOSÜSTEEMIDE INFOTURBE TAGAMINE OLUKORRAS, KUS PUUDUB ÜHINE INFOTURBE STANDARD

Magistritöö

Juhendaja: Alexander Horst
Norta
PhD

Kaasjuhendaja: Elin Iloste

MBA

Tallinn 2017

Author’s declaration of originality

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

Author: Maris Järvsoo

10.05.2017

Abstract

This Master's thesis analyses the EU information systems' security in a situation, where there are multiple regulations, directives, guidelines, but the unified standard, which shall be applied in development of Member States' subsystems is absent.

To conduct the analysis, existing documents are analysed and interviews with the specialists were conducted. For evaluation of the results the case study method is used. The cases analysed are chosen from the EU Internal Security and Justice area.

The main finding of the analysis shows that a separate standard is not necessary, but there is a need for setting minimum requirements, ensuring security of the information systems, as well as a necessity to prepare guidelines to help the Member States to achieve them. The second finding is that there is a necessity for greater cooperation and an increased knowledge exchange of the methods used in the Member States.

Following the guideline and exchanging knowledge would help to heighten the level of security for the entire system.

This thesis is written in English and is 35 pages long, including 5 chapters, 3 figures.

Annotatsioon

Euroopa Liidu infosüsteemide infoturbe tagamine olukorras, kus puudub ühine infoturbe standard

Käesolev magistritöö analüüsib Euroopa Liidu infosüsteemide turvalisust olukorras, kus on mitmeid regulatsioone ja juhendeid, kuid puudub ühine standard, millest tuleks liikmesriikidel IT arenduste puhul lähtuda.

Analüüsi läbiviimiseks vaadeldakse olemasolevaid dokumente ning viiakse läbi intervjuud spetsialistidega. Tulemuste hindamisel on abiks juhtumiuuring, mille läbiviimiseks kasutatakse kolme Euroopa Liidu siseturvalisuse ja justiitsvaldkonna infosüsteemi.

Peamise järeldusena selgus analüüsi tulemusena, et puudub vajadus eraldiseisva standardi järgi, kuid eksisteerib vajadus miinimumnõuete ning nende täitmiseks koostatud juhendi järgi. Ühtlasi tõi autor välja ka soovituse korrastada infoturvet puudutavad regulatsioonid ning rakendada otsuste vastuvõtmisel subsidiaarsusprintsiipi.

Teiseks järelduseks on vajadus suurema koostöö järele, mis võimaldaks efektiivsemat teadmusvahetust liikmesriikide poolt kasutatavate turvameetmete osas. Juhendi jälgimine ning teadmusvahetus aitaksid tõsta süsteemi kui terviku turvalisuse taset. Juhendi koostamise vastutus peaks lasuma EU-LISA-l, et tagada paindlikkus ning selle täiendamine vastavalt vajadusele.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 35 leheküljel, 5 peatükki, 3 joonist.

List of abbreviations and terms

ENISA	The European Union Agency for Network and Information Security
ETIAS	The European Travel Information and Authorisation System
EU	European Union
EU-LISA	European Agency for the operational management of Large-Scale IT Systems in the area of freedom, security and justice
EURODAC	European Asylum Dactyloscopy Database
EUROJUST	The European Union's Judicial Cooperation Unit
EUROPOL	European Police Office
GDPR	General Data Protection Regulation
IDA	Interchange of data between administrations
ISKE	Three-level IT baseline security system
IT	Information Technology
NIS	DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
SIRENE	Supplementary Information Request at the National Entry
SIS II	Schengen Information system II
TESTA	Trans-European Services for Telematics between Administrations
VIS	Visa information system

Table of contents

List of figures

1 Introduction

As the time goes by, information and communication technologies (ICT) systems get increasingly sophisticated while demanding more qualification from people who develop and operate those systems. (Li, Xie, Gui, & Ding, 2010, p. 1). On the other hand, different aspects of life depend highly on ICT, which means that the development has to be fast and agile while downtime regarding some systems is not acceptable. This paper focuses on the large-scale information systems, operated by the EU-LISA, the European Agency for the operational management of Large-Scale IT Systems in the area of freedom, security and justice, that helps to manage the border crossings and asylum requests to secure the Schengen Area.

The discussions regarding the information systems (IS) security level all over the EU have risen regarding the compilation of The Directive on security of network and information systems (NIS) directive, where the low level of security was pointed out. To increase the level of security, one of the measures highlighted, was to implement internationally accepted security standards. The directive is not specifying the standard that shall be taken into use. Author goes further with the idea and analyses if there should be one specific standard covering the security of the EU information systems. There have been discussions in EU about creating a standard for information security.

In the analysis, the author looks through the existing regulations and analyses them together with the specialists, who are implementing the requirements from the regulations. The aim is to find out if the existing regulations are sufficient in ensuring the security of the whole system including the central system or should the centralised approach to standardisation be taken into use.

1.1 Context

Since the formation of the European Union, its main goal has been a free market, freedom of movement and residence. In 1985, the Schengen Area was established and borders between the EU Member States exist only on a map. This means that citizens from

Member States of the Schengen Area can move freely, without any border control between European countries. The border control exists only on the external border of the Schengen Area. (European Commission & Directorate-General for Migration and Home Affairs, 2015)

There is a saying in Estonian which means in translation "Responsibilities always come with freedom". In this case, the members of the Area have to make sure that travellers from the third countries, who are entering the Schengen Area are people with good intentions and without criminal background. This is extremely important because the entering point to the Area might not be the same as the travel destination, so it is quite easy to cover the tracks and hide the real intentions. There are precedents that illustrate the negative effects of the free movement– for example the Berlin terror attack that occurred in 19th of December 2016. Attacker responsible for driving the lorry into the crowd in Berlin, Germany - was later found in Milan, Italy. (Kirchgaessner, 2016) This example illustrates, how fast and easy it is to travel to another country, even in a situation of heightened security risk. The other point of view, which this example illustrates, is the cooperation between security institutions in EU.

The cooperation is the crucial part in the context of free movement. Cooperation is not only physical, as information sharing is a part of it. Therefore, the European Commission has requested the development of information systems, which share and control the information of travellers. The main information systems' connecting fields of travelling and security are Schengen information system II (SIS II), Visa information system (VIS), European Asylum Dactyloscopy Database (EURODAC). Those systems share information between the Member States, allowing authorized personnel to process personal data and see if the person in question is flagged for some reason. To ensure the security in case of free movement, the European Commission created the authority named EU-LISA, which is responsible for developing previously named systems.(European Council, 2000; European Parliament, Council of the European Union, 2006, 2011; The European Parliament and the Council of the European Union, 2008)

The author uses previously mentioned three systems as examples for the research, they all are storing personal, including biometric data. Considering the number of states, 26(VIS), 29(SIS II), 32(EURODAC) and authorities within those states that have access to those systems – broad number of people can access that data. (European Council, 2000;

European Parliament, Council of the European Union, 2006; The European Parliament and the Council of the European Union, 2008)

In addition to ensuring the security of the citizens of the Member States, the security of the person crossing the borders or checked in other circumstances shall be assured. Therefore, the security of the systems is an important topic. Good learning point is the case when Danish authorities found out in 2013, that their information from national interface has been leaked. The discovery was made after the Swedish officials turned to Danes regarding their investigation. It turned out that the same hacker was involved in both cases and about 1.2 million records with personal data from SIS information system were found from the hackers' devices. Hacking took place in summer of 2012 and without the Swedish investigation, finding out the leakage would have taken longer. None of the systems alerted Danish officials about the problems. Luckily according to the investigation none of the personal data was harmfully used. ("Data Protection: unauthorized access to personal data in the systems that the National Police is responsible for data for," n.d.)

This example illustrates what could happen if the Member States systems are not secured sufficiently. Impact in this case was minimal since the data was not used for nefarious purposes but in data protection, unauthorized access to the personal information cannot be tolerated.

1.2 Problem statement

Importance of the topic proceeds from the implementation of the NIS directive, which comes into force in 2018. In the NIS directive, the need for the usage of information security standards is stated, leaving open the choice of the standard.

During the idea collection for the thesis, the author discussed the topic with multiple co-workers and with a supervisor, who are working on an internal security field and specifically with the EU information systems. One of the specialists was also from the EU side, the representative of the EU-LISA.

The topic is personally important to the author because in authors' everyday work is about ensuring the internal security in cooperation with the EU institutions and implementing EU regulations.

The one issue all the interviewees brought out was ensuring the information security of the systems. Despite the efforts by the EU-LISA in helping the Member States to gain the needed level of information security, the assurance for the parties is not ensured. Problems with the security mentioned during the discussions were:

1. Fractioned understanding and skills about the security of the large-scale information systems.

2. Multitude of methods ensuring the IS security used by different Member States.

3. Lack of collaboration and willingness to share or accept the knowledge of others.

According to the problems that were mentioned author started to think if different standards cover all the aspects necessary and are all the different standards and regulations equal in ensuring the security of the EU central system.

1.3 Research objective

The discussions with the supervisor, co-workers and representative of the EU-LISA lead to the point where the specialists did not have consensus regarding the question. Some of the interviewees and discussion partners are afraid if the EU starts strictly regulating the requirements, if the new regulations are as high level as some Member States already have implemented or vice versa – are other Member States able to implement the new requirements. The others thought that it would be a good idea to equalize the security measures and through that ensure the security of the central system.

To be able to analyse the main question, the first research question was created:

- How are the system requirements managed?

The contrasting point of views led to the second research question:

- "How effective are the current regulations, how many of those are mandatory and how is the implementation by Member States monitored?"

The answer to the second question helps to answer the main research question:

- Whether the EU needs a unified standard on ensuring information security of large-scale information systems?

An author proposes that:

- If requirements of the information security are standardized, then the security of the central systems is ensured through the equally secure methods used by all the parties.

Based on the previous discussions and readings author sets a hypothesis:

- Standardized approach is necessary to gain the equally high level of security for the EU large-scale information systems.

To be able to answer to the research questions, the documents related to the security will be analysed and secondly, the experience of the specialists directly connected to the systems will be collected. For the experience collection regarding the development and operation of the IS, the interviews were conducted. The conclusions and suggestions are done based on the comparison of the existing documents and the specialists' experiences.

1.4 Thesis structure

The thesis is structured into chapters from which Chapter 1 Is the introduction to the topic, Chapter 2 covers the theoretical approach and background description, Chapter 3. describes the methodology, Chapter 4 analyses the data and in Chapter 5, conclusions will be made.

In Chapter 1, the introduction of the relevance is brought out and the context is described, which will be followed by the problem statement and research objective. In the Research objective, the research questions and hypothesis are set. In the end of introduction, the thesis structure is given.

Chapter 2 gives an overview about the systems used as the case studies, as well as the EU, responsible for the operational management of those information systems. The theoretical framework described is about the Large-scale information systems, data exchange, data protection and standards.

In Chapter 3 the case study methodology is elaborated and the data collection and analysis process is described. In the end of Chapter 3, the validity of the analysis process is analysed.

In Chapter 4, the analysis is conducted. The analysis process is divided according to the research questions and themes. Inside every sub-chapter, the document analysis and interview analysis are brought out separately. The end of every subchapter the conclusion part ties the both analysis together.

The fifth, as the last chapter, concludes the findings and gives the suggestions for the further work, based on the limitations, which occurred in current research.

2 Theoretical framework and background

This chapter describes the information systems, that form the basis for the analysis, gives an overview of the standardisation and opens the background regarding the data exchange and protection.

There are a few earlier studies conducted on the topic of the current thesis. The most similar is the study conducted by the RAND corporation, which researched the EU information systems security and data protection from the legal and policy aspects, analysing the regulations applying to the EU authorities. The research focused on the creation of legal and policy frameworks and the possible effects on the information security in the EU.(Robinson & Gaspers, 2014)

2.1 Security of Large-Scale information systems

Large-Scale information systems are systems that contain multiple components and affect many users. By architecture, the system contains millions of lines of code and the system might be distributed in different geographically located sites.(National Research Council, 2000, p. 99-100, 108; Vithanage & Wijayanayake, 2007, p. 1) The control mechanisms of the Large-Scale ISs are usually distributed over multiple entities, as each subsystem is developed and controlled by a separate authority. On the one hand, this solution offers flexibility in case of errors of one subsystem, as the others will remain operational, but on the other hand, central control over the system operability is lacking of control. (Zheng, Li, & Li, 2011) The complexity of information flow and network, such as the connection of the components, is the main reason, why the Large-Scale ISs are complex. (National Research Council, 2000, p. 99-100, 108; Vithanage & Wijayanayake, 2007, p. 1)

The IS used as a case in this paper has a central system as a master and a set of horizontally distributed and replicated databases connected to it. Member States systems operate only with the replicated local data and connect to master using communication infrastructure to transmit data to the master. (Booth, 1976)

Ensuring the security of the information in distributed systems is about the encryption on authentication and access management processes. For the encryption, the methods based on public-private keys can be chosen e.g. RSA, PGP, DES. The access management

includes the authority and authorisation. The first is the hierarchical level of functionality, which the user can operate in, and the second is the specific field, which the user operates in. In this case, the authorisation may include the vehicle information from SIS II IS. (Armoni, 2002)

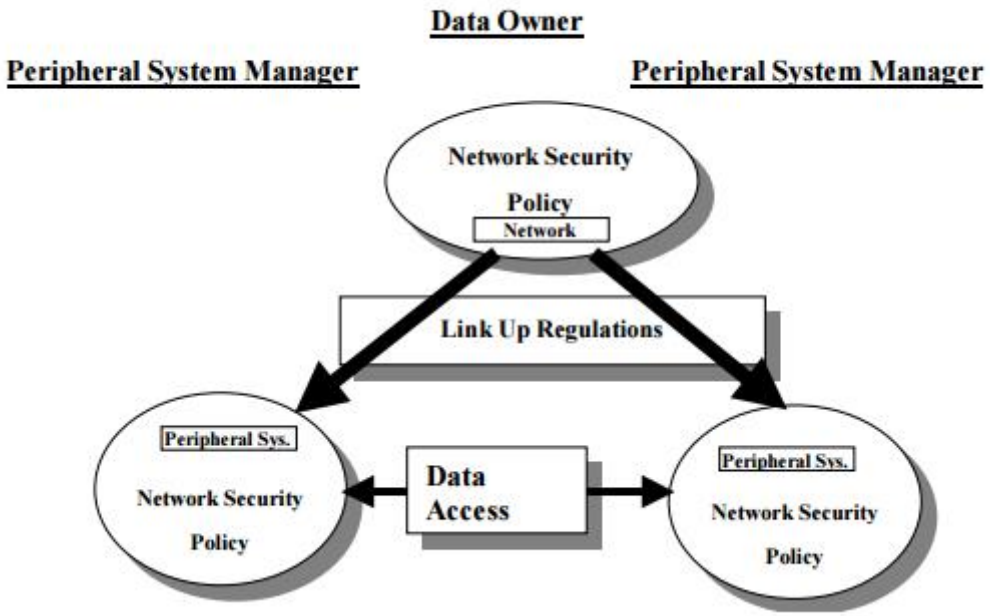

Figure 1 The Distributed Security Approach (Armoni, 2002)

In this paper considering only the Large-Scale IS under the control of the governmental authorities – the IS must fulfil the functions of holding and operating with personal data, and therefore the systems shall be secure and operate exactly in an extent they were built for, without compromising the availability and reliability. Systems operating with personal data shall be compliant with the data protection requirements, to ensure that the information is accessible only for the authorised personnel. The most difficult part in ensuring the trustworthiness and security is the human factor, which is hard to solve only on focusing on the systems' technological problems. (National Research Council, 2000, p. 114-115)

2.1.1 EU-LISA

EU-LISA is the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, established in 2011. The authorities' responsibility is the preparation, development and operational management of the information systems SIS, VIS and EURODAC, considered as a Case Study in this paper.

The systems under the responsibility of EU-LISA must be operational every day of the year and 24 hours in a day. The other responsibilities for EU-LISA are ensuring data and systems continuity, security, integrity, availability and compliance with data protection rules and European Commission regulation 2017/46/EC and training of the national authorities. To serve the task, EU-LISA needs to collaborate with National Systems providers and Data Protection supervisors and with the security officers network. (Council of the European Union, 2016; European Commission, 2017; Zampaglione, 2017)

The need for the specific authority was triggered, among other reasons, by the development process of SIS II, which was originally under the responsibility of the EU Commission, but as the European Court of Auditors brought out – there was not enough knowledge involved into the process, which lead to the extension of the process and eight times higher budget than planned. (European Court of Auditors, 2014 p6, 41)

2.1.2 EU Information systems

The three main information systems under the responsibility of EU-LISA have a common task of storing personal data, including biometry.

The Schengen Information System (SIS) core function is information exchange between national border control, police and customs officials. The information exchanged contains alerts about persons - missing persons and children for example, also information about stolen and lost documents and property – money, vehicles, firearms. (European Court of Auditors, 2014, p 8)

EURODAC system is an instrument to full-fill the requirements of the Dublin Convention (now: regulation) which helps to compare fingerprints, to find out if the person has already applied for asylum in another Member State or stays at the state illegally. Therefore it helps to avoid outwitting the European law by being rejected in one Member State and trying to get the asylum in another – called “asylum shopping”. (European Commission, 2003; European Council, 2000; Secretariat of the Eurodac Supervision Coordination Group, 2009)

VIS serves a purpose of improving the visa policy and better cooperation between Member States, specifically enables the facilitation of the checks at the external borders

of the Schengen Area. The purpose is gained by the following tasks VIS serves: proceeding the visa applications, controlling the person and its visa against the system during the border crossing, helping to manage asylum requests, identification and checking if the conditions for entry, to stay or residence are fulfilled. (The European Parliament and the Council of the European Union, 2008)

The main parts of the information systems described previously are the central systems which consist the database and uniform national interfaces. Every Member State operates, maintains and is responsible of developing the national systems, which are holding the copies of the central systems. The national copies are for conducting automated searches on Member States' territory. The data will be entered to the central system. It is not possible to search data from another Member States' national interfaces. There is a communication infrastructure between central systems and national interfaces – for information transfer and conducting searches. The Communication Infrastructure provides encrypted network for the data exchange. (European Council, 2000; European Parliament, Council of the European Union, 2006; The European Parliament and the Council of the European Union, 2008)

According to the IS regulations every Member State shall have an authority responsible for operating the national interfaces, assuring the security and compliance with the instructions from the regulations.

2.2 Data exchange and protection in a field of police and justice

In the field of police and justice that by its nature requires processing of sensitive personal data - consequences in the case of data leakage or other ways illegitimate use of data might result in violation of privacy or personal harm. The field covers the areas of police and border control, asylum and immigration, judicial cooperation in civil as well as in criminal matters and police cooperation. (Boehm, 2012) Therefore, this field needs a tailor-made protection methods for data protection in the large-scale information systems of the EU. The Data Protection Directive 95/46/EC in force, is not making difference in different fields of data usage, therefore the protection of the personal data operated in a field of police and justice is not regulated specifically, but it follows the overall regulation. The directive is not applying to the processing of the personal data outside of the boundaries of Community law. Despite that, the Member States have widened the

scope of the directive during the engagement of the directive to the national law. (Alonso Blas, 2010; Marquenie, 2017)

The need for the specific regulation for the police and justice field was acknowledged already in 1987, by the council of Europe. Since then the provisions have been adopted and in 2005 the Krakow declaration was adopted, with the official name of the paper: Law Enforcement & Information Exchange in the EU. Before the Krakow declaration the Europol adopted the Eurojust Decision where the detailed framework regarding the data protection and operation in police authorities was brought out.(Alonso Blas, 2010)

Since the 9/11 terror attack in United States of America, the information transmission from one field to another has risen and the information collected in specific purposes might be transmitted to another field and used in other purposes. This is a risk in terms of data protection and is not in accordance of the principles of integrity and human rights, therefore tensions between the data protection and ensuring the security have risen and Data protection officials shall work on regaining the balance between both important point of views. (Boehm, 2012; Marquenie, 2017)

From the security aspect the large-scale information systems contain large amounts of data, which risk of abuse rises with every data processing (Boehm, 2012). The more officials and authorities have the access to the information, the bigger is the risk of entering the incorrect data and not be able to correct it before this might affect the person in other situations; for example, the visa application process might be more difficult if the SIS II IS contains a note about the person or the police might use the expired information during the discretion process.(Boehm, 2012; Marquenie, 2017) These problems can be solved by applying strict access management processes e.g. task-oriented access, in the authorities having the access to the data processing. (Rull, Täks, & Norta, 2014)

With the new Data Protection Act (GDPR), the focus regarding data protection in the information systems lays on the minimisation of the collected data. Therefore data protection shall be considered in the IS development. Additionally, data protection should be implemented by design, e.g. by measures such as “data protection by default”. The GDPR set contains a directive regarding the data processing for the prevention, investigation, detection and prosecution of criminal offences, which is tailor-made tool

of data protection for the police authorities. (European Parliament, Council of the European Union, 2016b)

2.2.1 Data exchange and protection requirements for EU Information systems

Personal data protection is regulated primarily by the EU Data Protection Directive (94/46/EC), which will be replaced with the GDPR in 2018 (2016/679/EC).

Exchange of the supplementary information of SIS II and VIS, between Member States and Central units goes according to the SIRENE manual, regulations and through communication infrastructure TESTA. EURODAC data is transferred between the Central Unit and Member state by using TESTA. (Commission of the European Communities, 2004) TESTA II is (Trans-European Services for Telematics between Administrations) infrastructure which is a virtual private network over public internet meant for public administrations. (Commission of the European Communities, 2004; Li et al., 2010)

TESTA II was upgraded to a sTESTA, which is third generation system. In 2006 and in 2013, the fourth generation was brought into live TESTA NG. (Wellens, 2013) TESTA can be used to exchange both classified and unclassified information. This is made possible through the implemented IPsec technology and cryptology measures. TESTA value chain is brought out on the Figure 1. (Robinson & Gaspers, 2014)

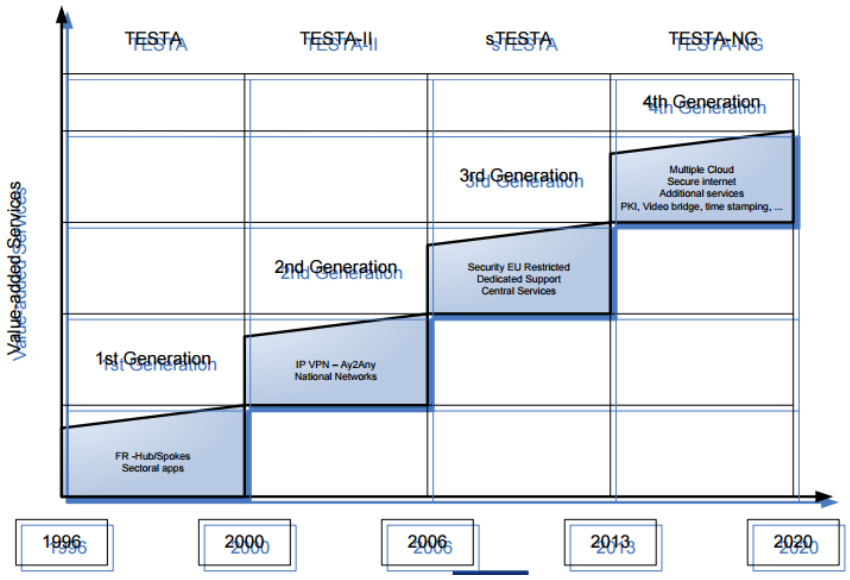

Figure 2 TESTA value chain (Wellens, 2013)

In case of the situation when the communication infrastructure cannot be used, the Member States can use sufficiently secured other data and information exchange channels. To make sure that the information can be transmitted to the authority, the security plan must contain the communication control protocol, where the requirements of the accepted authorities is listed. (European Parliament, Council of the European Union, 2006)

Personal data transmission and making the data available to the third parties as international organisations or third countries is prohibited according to the IS regulations. (European Council, 2000; European Parliament, Council of the European Union, 2006; The European Parliament and the Council of the European Union, 2008)

Every Member State applies necessary measures to make sure that transmitted and processed personal data is not leaked and available for unauthorised authorities or people. The 95/46/EC (from 2018 GDPR 2016/679/EC) stipulates that assuring the lawfulness of the data processing procedures and helping to solve the questions of people regarding the personal information held in the EU IS, Member States shall have the independent Supervisory authority. The National Supervisory Authority conducts an audit once in every four years to validate if the data processing in national interfaces is done according to the international standards. EU Data Protection Supervisor conducts audits once in every four years to make sure that personal data in central systems is processed according to the regulation and international standards. To ensure the coordinated supervision, National Supervisory Authorities and EU Data Protection Supervisor meet after every half year to discuss the problems, exchange the information and unify the regulation. (European Parliament, Council of the European Union, 2006, 2013; The European Parliament and the Council of the European Union, 2008)

2.3 Standardisation

In the Business Dictionary, standardisation is defined as follows: "*Formulation, publication, and implementation of guidelines, rules, and specifications for common and repeated use, aimed at achieving optimum degree of order or uniformity in a given context, discipline, or field.*" ("What is standardization?," n.d.) According to the definition, standard is a rulebook that sets the minimum requirements to ensure the

security of the system. For information security, there are many standards or guidelines, that are also used by the public sector, like ISO 27 000' series, ISKE, ITIL, *IT-Grundschutz.* The standards alone would not ensure the safety of the systems. Instead, they offer a framework where to operate and gain the best outcome.

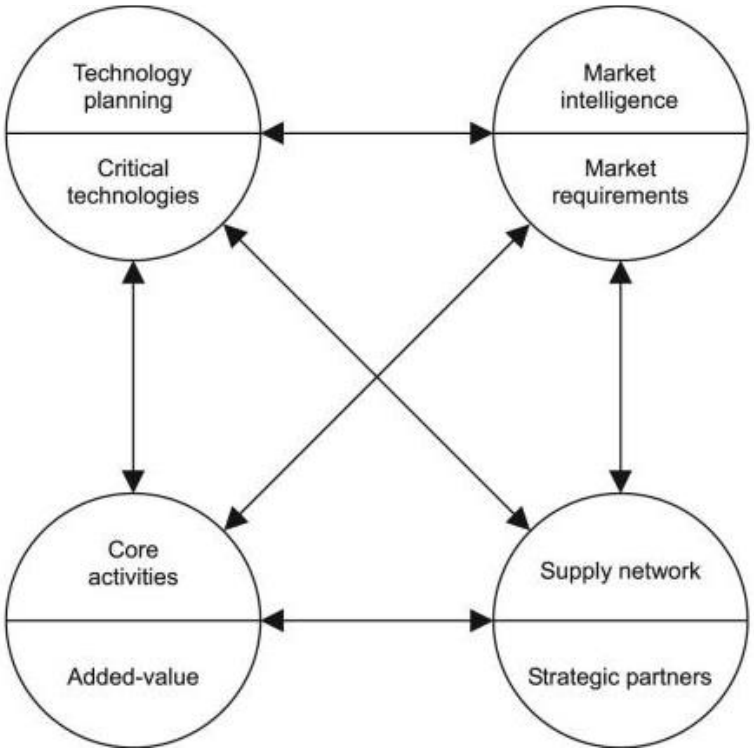

Figure 3 Critical factors in the implementation of standardisation (Gudmundsson, Boer, & Corso, 2004)

Previously set standard is a tool that points out the possible problems and helps to prevent their occurrence. In addition, standard gives a baseline to operate within and therefore, helps to ensure the continuity and accuracy of the development process and helps to prevent delays of development. (Gudmundsson et al., 2004)

The aim of the standardisation is helping to reduce time to market, within the solution will be operational, through setting the strategy and thinking thoroughly about the tasks and planning the resources. (Gudmundsson et al., 2004) Time to market in IT security development is crucial to prevent the attacks or data breaches. The resource planning covers financial and human resources, planned to use during the development process. Comprehensive plan helps to gain the higher quality of the outcome. (Gudmundsson et al., 2004)

3 Methodology

The chapter describes the analysis methodology used for the paper. The essential ideas for the topic were collected from the authority, where the author works, which is responsible for the Member State side of the systems, analysed in the paper.

3.1 Interpretivism as a research philosophy and qualitative analysis

The philosophy suitable for the analysis of the paper is interpretivism. Interpretivism was chosen because of its' essence to rely on a subjective experience of the small number of respondents. During the idea search, there were multiple people that this topic was discussed with, but the interviews were made only with the main specialists, because they are qualified to give an analytical overview. The interviewees were the security officer of the EU-LISA and two specialists who are working with the Member State systems. Therefore, those people have the most knowledge in Estonia about the systems and the operation of those systems.

The interviews are textual and cannot be interpreted to numeric values. Imperative philosophy of the research is illustrating the overview of the systems that, give a scope of the environment within the research is taking place. The research outcomes are illustrating the experience of the specialists and might not be accurate to generalise the experience to all the different Member States. Under the limitations and suggestions, the wider research necessity is brought out. This subjective coverage and generalisation regarding the scope illustrates the one approach of the imperative philosophy. (Williams, 2000)

The selected research approach is qualitative. The approach was chosen because of the theory-driven research and the aim to see the inside of the systems through the interviews. (Ritchie, Lewis, McNaughton Nicholls, & Ormston, 2014) The idea is to analyse the regulations of the systems against the experience of the system specialists from the Member States to find out if the information on paper is in accordance with the reality.

The empirical part is combined from the previous studies and literature and data analysis. Based on the qualitative analysis of the IS, commonly used regulations, the insight and problems pointed out by the specialists, the author proposes recommendations to the EU, regarding the security of the information systems according to the research questions and

hypothesis set for this paper. The empirical part of the research is inductive and exploratory. Inductive approach enables to use specific cases to analyse the situation and to widen the implications to the whole area of the police and justice information security. The exploratory case study has inductive characteristics, which help to find out what is the reality of the situation and to get the suggestions and find out about the needs for the improvements from the specialists. The exploratory research enables to give suggestions based on the outcomes for the future research. (Runeson, Host, Rainer, & Regnell, 2012) The empirical analysis is conducted based on the openly available documents from EUR-LEX information system and the information collected during the interviews.

3.2 Case study research and subject selection

The case study research is about analysing and comparing the existing information in a present context through which it is possible to create new solutions. (Yin, 2014) The previous description defines, why the case study is chosen for this paper. The paper is based on three large scale-information systems in EU, which are essentially similar, considering their security requirements, and therefore those information systems are considered as one case.

For the analysis of existing situation, the interview method was chosen, because the specialists have the necessary insights and experience and thus, should know the way forward. The sample for the interviews is small and selected based on the speciality of the interviewees.

The interviews were conducted in-person with the duration from an hour to two hours, depending on the interviewees. The interview was held in form of an open discussion, where the topic "IS security reality regarding SIS II, VIS and EURODAC in comparison of the regulations" was given. The topic was previously presented at the time of arranging the meeting, so the interviewees had time to prepare. The main condition to bear in mind was that the research is open, and therefore the classified information was not permitted to be shared during the interviews. This point was important because of the author's connection with the authority and therefore the existing access to deeper knowledge.

All the interviewees had the opportunity to decline and after the interviews they had the opportunity to read the transcripts and make changes to ensure the validity of the

information gained. During the analysis process, some additional questions arose, which were answered via the e-mail.

3.3 Data collection and analysis methods

3.3.1 Data collection

The data collection can be divided into two subsections. First part is the empirical information about the systems under analysation. The second part is the interviews, conducted with the specialists.

Empirical data collection methods for the paper can be divided into two: Independent and direct. (Runeson et al., 2012, p 32)

The independent method is used for the documentation analysis. (*Ibid.,* p. 32) The descriptions of the systems and existing strategies are the basis for the analysis done in the paper and they form the essence of Case Study. The data was collected mostly from the internet and more specifically EUR-LEX information system, that contains all the EU legal documents. Some of the documents were gained from the interviewees as well. Academic articles and previous studies were found from Google Scholar and Ebscohost system.

The European Commission has set the system requirements for the security and the EU-LISA together with the Member States must carry out those requirements, by using the existing standards or best practices available. To get the insight to the reality, open interviews with the given topic were carried out. More specifically, the direct method is used, when analysing the experience and the actual situation based on the interviews. (*Ibid.,* p 32)

The interviews are conducted to get the insight from the people working with the IS daily, to offer an opinion about the regulations and their aptitude with the needs of such systems. The interviewees are the main supervisors from the Member State side, therefore responsible for the operations and developing the information systems. There are only few people connected to those systems in Estonia?!, therefore the number of interviewees is limited.

To compensate the small number of the interviewees from Member States, the interview with the person responsible for the security of the central system was conducted. The security officer has the knowledge about the whole system, and therefore he could give the insight from both sides and comment on the cooperation between Member States.

The data collection occurred within the timeframe of January 2017 and April 2017. At the same time period the interviews were conducted as well. Groundwork that was needed for the interviews was made in December 2016.

3.3.2 Analysis process

The analysis procedure can be divided into two – first, the document analysis, based on the regulations of the systems, existing internationally accepted standards and guidelines and previous studies. The second part of the process is interview analysis.

Both documents and interviews were analysed according to the thematic analysis concept. Thematic analysis was chosen for this paper because of its suitability to analyse the contrasts and similarities in qualitative research. The method gives a specific guideline to sort out the necessary information by categorising it according to the research topic. (Vaismoradi, Turunen, & Bondas, 2013)

The document analysis was conducted on the paper, because of the authors preference of working with the paper documents. The interviews were transcribed and after the validation by the interviewees entered to the NVIVO tool for further analysing. The NVIVO tool was selected to help to compare and select the information without losing some of the answers. For the both analysis, together over 100 nodes were created, but only 34 were used further. The 34 nodes were divided under the themes: security, data exchange, cooperation, strategies and management. To help to structure the themes for the document analysis, colour coding was used, where each theme responded to specific colour of the post-its.

The security theme consists the nodes about the security regulations, personnel, security plan. The data exchange theme is about the regulations, policies, tools used to ensure the secure exchange and the data, that is exchanged. Cooperation theme is about cooperation between Member States, Member State to Central and vice versa and knowledge

exchange. Theme about strategies covers the data exchange security aspect. The management theme covers all the areas that are about policy making.

3.4 Validity of the data and process

The information that was collected originates from the official materials of the EU databases or from the academic articles. The data collected for the document analysis is publicly available and satisfies the purposes of this research. To conduct further research on the topic, it is important to gain access to the classified information, security plans and technical structure of the systems.

To offer a credibility specialists from both sides of the systems were interviewed – central system and Member State representatives. For further research, it is important to contact other Member States' representatives from different maturity levels regarding information security. Similarly, the previously conducted researches in other Member States illustrate their experience regarding EU information systems and their development, based on which the aggregative research can be done. At the request, the interviewees' names are not published.

During the analysis, similarities with the RAND corporations' research findings were detected regarding the information systems in a field on internal security and justice. The main similarities were the finding about the federated management of the information security and data protection through obligatory measurements like regulations.

4 Analysis

In this chapter, the author analyses the findings regarding the research questions. Analysis part in each subsection is divided into two, based on the collected data. First the document analysis is conducted and after that the interview outcomes are discussed. Interview analysis in each chapter is divided into two – first the insight from the EU-LISA and then from the specialists the Member States.

Subsections follow the logic of the research questions therefore; first subsection analyses the policy-making and management of the systems. The second subsection is about the security in data exchange between the central system and Member States' subsystems and answers the second research question.

The third subsection answers the main research question through analysing the internationally accepted standards and guidelines and comparing the results with the interview outcomes. By answering the main research question the result of the proving of the hypothesis set by an author, will be elaborated.

4.1 Policy and management

4.1.1 Introduction

In this chapter, the analysis of policy making and management process of the EU IS is conducted. The first research question will be answered, by analysing the EU legal documents and interviews conducted with the specialists. The interviews are analysed to pass on the experiences and shortcomings of the legal process. The themes created in NVIVO for analysing this topic were "management" and "cooperation".

4.1.2 Document analysis

4.1.2.1 Management of the Information Systems

The overall security measures of EU are covered with the EU Commission decision about the security of the information and communication systems in responsibility of EU Commission. EU regulation 2017/46/EC sets areas of responsibilities to different groups and authorities of EU. Altogether, the regulation brings out nine different authorities and groups with their areas of responsibilities. The authorities are listed hierarchically, which

means, that every lower authority and group reports to higher and some of the responsibilities are fulfilled together. Every authority monitors the execution of some areas of the strategies or policies and creates the frameworks within the service providers or national authorities must work in. The access to the cryptology measures is given by the Directorate-General Human Resources and Security and the access is asked by the System owners. Five of the nine authorities are creating strategies, frameworks and policies, three groups – system owners, data owners and LISOs (Local informatics security officers) are giving input to the guiding documents and the last group – users, are obligated to follow the rules and recommendations. (European Commission, 2017)

The EU directive 2016/1148 is aim is to gain a commonly high level of security of network and information systems across the EU (NIS directive). Therefore, the directive focuses on public-private cooperation and sets the requirement for the Member States to establish an information security strategy. The main concerns are security incidents and having an overview of them. Every Member State must to have an authority managing the information security incidents – CERT. To gain the commonly high level of security, NIS directive sets the reporting obligation to the Member States and the CERT authorities to the EU Commission, about the condition of the IS and the incidents taken place. Commission evaluates after every two years the execution of the directive. In addition to the CERTs, every Member State shall name one authority that would be the contact point for the EU Commission to get the information regarding the authorities and IS of the state. The contact point is also responsible for evaluation and application of the directive. (European Parliament, Council of the European Union, 2016a)

As the directive comes to an effect in 2018, the reporting obligation expands on every service provider – public or private, who operates with the critical infrastructure and internationally vital services. The NIS directive points out the need for common ground and understanding of the systems' security - which is considered as a foundation to gaining an equally high level security for all the information systems. (European Parliament, Council of the European Union, 2016a)

Every IS has system specific regulation that sets the frames for the system security and its supervisors, issued by EU Parliament and the Council of EU. The systems SIS II, VIS, EURODAC, are under the EU-LISA responsibility, which is reporting to the EU Commission. EU-LISA is responsible for the development and operation of the whole

large-scale information system and directly of the central system. The Member State systems are developed and managed by the Member States, that are obliged to follow the directions of the EU-LISA and EU Commission. The lawfulness of the information processing is reviewed by the Data protection offices of the Member States and the Central systems are controlled by the EU Data Protection officers. (European Council, 2000; European Parliament, Council of the European Union, 2006, 2013; The European Parliament and the Council of the European Union, 2008)

4.1.2.2 Cooperation

NIS directive sets a finger on a shortcoming that prevents the growth of the security level, through recommending a higher level of cooperation with the relevant authorities in Member States and EU authorities as ENISA. The recommendation to the EU Commission is brought out as well, which contains the suggestion to cooperate more with ENISA and consult with the interest groups in policy making and improving. (European Parliament, Council of the European Union, 2016a)

Regarding SIS II, which is the biggest information system in EU, in addition to the system regulation the SIRENE manual was created, to set the boundaries to the operations done by the Member States. SIRENE bureaus are the main contact points to every official operating with the information entered to the SIS II IS. Through the SIRENE bureau the cooperation with EUROPOL, EUROJUST and INTERPOL is organised and the announcements are done. All SIRENE bureaus are cooperating with each other, to operate with the information entered to the IS in the level of its needed to solve the issue, why the information was entered. (European Commission, 2015)

4.1.3 Interview analysis

4.1.3.1 Management of the Information systems

Contact from EU-LISA finds that despite the requirement of compiling security plans and setting the specific rules inside the State, there are Member States, that are not able to conduct the specific security plan. Some of the States are able, but not willing, therefore the quality of the security plans is lacking and based on them it is difficult to make management decisions. To help Member States to raise the level of security knowledge and ability to develop the measures themselves, EU-LISA is working on a security and continuity management system, together with the business continuity plans and security incident management procedure, to make them more acceptable to the Member States,

that they would see the need to use those templates and through that grow their knowledge about preventing incidents and avoiding them to happen. The templates are being renewed together with the EU Commission, to ensure that their requirements are still satisfied. The requirement from the NIS directive is that all the Member States would use a standard to help them prepare the security of the systems and therefore those templates are being renewed to be compliant with the ISO requirements.

The Member States are aware of the need for the security plan, but the need for them is taken more as a requirement, that shall be done, but not as a strategic planning paper, that could help them to ensure the growing level of security. Member States are following more the inner State requirements and standards, as ISKE in Estonia.

From the Member State side the management of the systems is bureaucratic, but they also see, that large-scale information systems as used as a case, shall have some level bureaucracy written in to ensure the continuity and prevent the falling apart. In this case, there could be less paperwork, which helps to work with the developments faster. Every aspect shall be discussed to ensure the similar understanding, but the accepting rounds could be shorter. Every bigger change shall go through the Change Management Group for final agreement, but before that the discussions are held in working groups, after that in Advisory Groups, from which the first is focusing on the business side of the system and the other is technical group. The process through each group is long and takes a lot of time.

All the procedures are very detail form regulating the letter subject to the forms shall be used and wording shall be chosen to address the questions. There are different levels of communications and to reach the next level, whose task shall be the problem resolving of specific case, the first level must be used and after the evaluation of the process on the first level, the permission to turn on the next is given. This is the biggest problem in working with the development of the systems, because it takes a lot of time and as system specialist see, it is a bureaucracy in its' worst meaning. If those processes could be easier the whole work can be faster and easier questions would get the answer only by contacting directly to the right officials.

4.1.3.2 Cooperation

The cooperation between Member States and central coordination organisation is not as good as it should be. The cooperation is based on the required meetings and paperwork, that shall be done, but there is no open discussion, to help the whole EU system to improve. To start the open discussion the Security Officers Network (SON) was created, where every Member State could share the experience and therefore help out the others that are falling behind or gain the knowledge needed to improve their own systems. The attitude is hard to brake; therefore, the SON is still working as a mandatory meeting, not as the open discussion round. Required security plans are presented, but some Member States are trying to write the paper as overall as possible or as they assume the EU-LISA would like to see it, to prevent further questions and discussions. The reality might not be compliant with the information presented on the paper. According to the EU-LISA experience, some of the Member States are working hard to be independent and not give any information out to the EU, which makes ensuring the security of the central system much harder, because of the lack of knowledge, what is going on in a Member State system.

The cooperation between Member States has been getting better over the time. The unofficial meetings have started occurring, where the developments are discussed. Usually the highlights are brought up in there, but there is a chance to ask for help if needed. There are also working Member States e-mailing lists where the necessity based communication is held. Despite that the communication could be better. The knowledge exchange is not working in daily bases, but the Member State initiated meetings could be a starting point for that.

The cooperation between some of the Member States is better than the whole picture. The example in here is the Estonian-Finnish collaboration in testing the systems.

The inhibitors for the active cooperation are the official meetings, where the officials of the EU Commission are also present including to the Member State representatives and EU-LISA. Those meetings are controlled and participants are holding back their thoughts. The presence of the EU Commission official is restraining the Member States, which was the reason of starting the unofficial meetings.

The cooperation between the EU-LISA and Member States are mostly good and the necessity is understood, but there have been problems over the time regarding the communication – where one party is not understanding the responsibilities or the central control has trouble in understanding the situation of Member States and therefore the advice they are giving is not suitable. Therefore, the Member State specialists are hoping that the inner process will be better soon, so the cooperation between EU-LISA goes smoothly.

4.1.4 Conclusions

The document analysis and interviews show that there are multiple levels of decision makers, which makes the decision process time consuming. The forms are created for the tasks, procedures of usage are set, but the importance and usage are still unclear. Documents like security plan, that should be helpful for Member States in planning their security strategy and for the central decision makers for seeing the continuity process and give a hand if necessary are not filling their purpose, because they are seen as a bureaucratic procedure.

On the other hand, some level of bureaucracy for managing the systems with the capacity as those is necessary. The level shall be looked over and updated.

The cooperation between Member States is still weak, but it has started to develop. The specialists see, that the cooperation between Member States will increase organically and that cannot be pushed, because by pushing it has the central control and it might lose its' focus.

Cooperation between the EU-LISA and Member States is evaluated as quite good and need for an organisation as EU-LISA is seen, but it has its' problems. The main problems are communication problems, when one party is not able to understand the needs of the other. The biggest problem is with the EU Commission, which is seen as a biggest inhibitor of cooperation. The official meetings where the EU Commission is present, the Member States are holding back their thoughts and are not willing to open discussions.

EU-LISA sees the problems also and on their side the main problem is lack of communication. The regulated reports are given, but the knowledge exchange and

unofficial communication is not working. EU-LISA tries to change the attitude and by creating SONs to induce the cooperation.

4.2 Ensuring security in data exchange and operation

4.2.1 Introduction

In this chapter, the documents regarding the data exchange requirements and security will be analysed. Specialists' interviews bring out the measures that are adopted and shortcomings that are not covered. The chapter answers the first research question: "How effective are the current regulations, how many of those are mandatory and how is the implementation by Member States monitored?" the themes for analysing this topic are "data exchange" and "security".

4.2.2 Document analysis

4.2.2.1 Data exchange and measures

In 2018, the new version of EU General Data Protection Regulation comes to an effect. The aim of the regulation is to unify the requirements of the Data regulations across the EU, which is important in case of free market and common IS. Under the new GDPR the directive is given out, which regulates the data protection in case of processing the personal information for purposes of prevention, investigation or prosecution of criminal offences and activities. According to the GDPR and its' directive the information can be processed only by the competent authorities and according to the rules set by the EU. The work of the authorities is controlled by the independent Data Protection Officers, whose role is to make sure that the personal information is used only within the frames of the regulations and the rights of the data subject are not affected. GDPR is relevant from the IS development side especially, because the new Data Protection regulation encourages the privacy by design approach, where the systems are already built according to the data protection requirements and in a way, that as few information is stored as possible to fulfil the requirements of the job. (European Parliament, Council of the European Union, 2016c, 2016b,)

The EU information systems must follow the current data protection directive and from 2018 the GDPR. All the information systems and their management shall be compliant with the principles of data protection set in those regulations. Regarding the information systems, used in the case, the personal data protection is vital, because of the nature of the systems. The collection of the data, storing and management has to be in correlation with the regulations. Data leakages shall be recorded, fixed and reported to the Data Protection Authorities and their recommendations shall be considered. On the other hand, the Data Protection officers are the help for the Data Subject, whenever data subject needs the consultation, the authorities shall give it and regarding the deletion and correction of the data authorities shall observe the rights of the data subject are fulfilled. (European Commission, 2015; European Council, 2000; European Parliament, Council of the European Union, 2006, 2013, 2016c, 2016b; The European Parliament and the Council of the European Union, 2008)

Regarding the usage of personal information, the authorities shall set the policies and the user profiles to enable the access only to the specific lines of information needed to fulfil the responsibilities of the work to prevent the leakages. In IS used as a case, the information shall be upgraded, edited or deleted only by the author of the entry and the changes can be required via the information exchange interface or SIRENE bureau. Data Protection officer intervenes to the change process if the rights of the data subject have been violated, or the data subject has the feeling they might be. (*ibid.*)

The information exchange in case of the systems used in the field of internal security and justice is according to the system regulations through the information exchange interface, which allows the secure communication with other authorities. The information exchange goes through the TESTA network, which enables also the exchange of the classified information due to the encryption possibilities. The supplementary information exchange in SIS II is organised through SIRENE bureaus, where the information exchanged shall be on the specific forms. In all cases the other channels may be used only in extremely urgent cases or if the information systems are not operational. (*Ibid*.)

4.2.2.2 Information security and measures

To ensure the security of the EU information systems the risks shall be evaluated and measures considered to prevent the risk realisation, therefore the regulation regarding the EU commission IS the responsibilities are divided between different supervisors, that

shall be ready to identify, prevent, report or create policies about the risks. The same regulation divides the responsibilities for developing and giving insight for the strategy and incident management. The groups and authorities are working in hierarchy therefore the lower level group is reporting to the group or authority in a higher level. The access management for the cryptology usage is managed by the authorities. (European Commission, 2017)

The NIS directives' aim is to achieve an equally high level of the information security all over the EU. To achieve that goal, it is important for all Member States to follow similar approaches regarding information system security. The NIS directive brings out the need for standardised minimum requirements and guidelines to achieve the outcome. The other important steps to gain the equally high level of security is the cooperation, information exchange and similar requirements for the public and private authorities who operate with the information systems regarding vital services. The NIS directive proposes every Member State shall have the national strategy for information security and policies to exploit. In addition to the national paperwork, the incidents shall be handled through the CIRT or CERT, organisations that handle the incidents and respond to them. In addition, CIRT and CERT are reporting to the EU, therefore there is a shared incident knowledge over EU. The NIS recommends the Member States to take into use some of the internationally accepted information security standards, to be able to equalise the level of security. (European Parliament, Council of the European Union, 2016a)

The system regulations bring up the need to put the managerial requirements and polices in place. The IS under the development or organisation shall have authority responsible for the security and in the authority the operation polices shall be implemented and presented to the EU Commission in form of security plan. The polices shall include the access management policies, which must be implemented for the physical locations where the information is held or where the systems are located and the digital security measures, which include the access to the systems and logging process. Another measure that helps to prevent the manipulation of the information across the State borders is that the owner of the information entered to the system is the Member State that enters the information at the first place and the other Member States shall transmit the information that should be implemented to the owner of the information, not implement it by themselves. (European Parliament, Council of the European Union, 2006, 2008 2013, 2016a)

4.2.3 Interview analysis

4.2.3.1 Data exchange and measures

The specialists are seeing the existing information exchange network as secure in general. The information is moved through defined channels according to the defined protocol in the interface control document. The protocol itself arises more concerns. Despite the existing interface control document, Member States implement sending of the forms differently and that can cause problems. Those problems are raised in the working group meetings and implementation details of the forms are being discussed. Solving those problems can be a slow process.

The physical environment security accordance to the regulations, is controlled by the local Data Protection Authorities.

4.2.3.2 Information security and measures

The security plans are mandatory, but the quality of the papers is hectic. This has many reasons, some of the States do not have enough knowledge to develop the complex security plans and systems, while some of the States are not willing to share the information to prevent the EU side questions and improvement suggestions. The variety in the quality is making the evaluation of the overall systems' security difficult.

Member States do not have the overview about the others' security measures and do not know, if and what the international standards are used. The security measures required by the EU are comprehensive and their implementation is controlled in every five years during the evaluation.

Specialists from the Member States see the security rules as strict, specifically the process described in the interface control document. Responses to some of the questions must pass multiple levels of contacts because of the right to access rules. Every level of contact has the information they are allowed to process and therefore it is not possible to get the answers from one level for some questions.

Specialists see some aspects as over regulation, for example if the report of the data usage and handling shall be done, then Member States must create their own reports, which will be combined by EU-LISA later, to present to the EU Commission, despite they have access to all the information stored by Member States and they could to it themselves.

This situation has been brought up at the working groups for many times, but the obstacle is regulation which is not allowing EU-LISA to operate with the information, that is held by Member States. Member States have all proposed, that they would give the mandate to the EU-LISA to manage the information for creating the reports, to lower their own administrative burden, but until now, that has not been changed.

4.2.4 Conclusions

On one hand security requirements by the EU are comprehensive, but grant enough freedom for the Member State to choose the measures suitable for their inner legislation. This leads to situation where overview about security measures used is lacking, despite the evaluations conducted. The evaluations are Member State specific and are not compared to see their compatibility to each other. Request brought out in NIS directive should give a clearer overview, if all Member States would use the internationally accepted standards.

On the other hand, some aspects are over regulated, which leads to the administrative burden.

4.3 Usage of standards

4.3.1 Introduction

This chapter analyses the aspects that, internationally accepted standards and guidelines are covering. Specialists are giving an overview of how the standardised framework is affecting their work and propose ideas how to make their work easier. This chapter the answer for the main question of the research "Whether the EU needs a unified standard on ensuring information security of large-scale information systems?" is found and hypothesis "Standardized approach is necessary to gain the equally high level of security for the EU large-scale information systems." will be proved. The theme created for analysing the topic is "standards".

4.3.2 Document analysis

The regulations about the information systems are not regulating the need for the official information security standards. The first time the need for the usage of internationally accepted information security standard is pointed out is the NIS directive article 19, where

the recommendation is to adopt the standards, to reduce the amount of the different approaches used to ensure the security of the system, but the directive does not detail require, which standard should be used. (European Parliament, Council of the European Union, 2016a)

The information systems' regulations use the similar requirement for the systems security, but those requirements are high level and are not setting the guidelines how to fulfil the requirements. The term "standard" is used in SIRENE manual, where the basic requirements as acceptability, continuity, confidentiality and access are described. (European Commission, 2015)

The internationally used standards such as ISO27001, guidelines as ISO27002 and base line standards as IT-*Grundschutz* and ISKE are used. The ISOs are directed more to the information system management systems and their requirements, the polices that shall be implemented in the organisation and less to the security of the systems itself, whereas the baseline standards are directed to both. The ISO requirements are in accordance to the requirements set by the EU regulations – require the risk assessment, policies for access and operation of the systems. The base line standards evaluate the information systems based on the information stored in the systems, users and field of usage in addition to the managerial policy requirements. (British Standard Institution, 2013; Bundesamt für Sicherheit in der Informationstechnik, 2007, 2016; Eesti Standardikeskus, 2017; "Infosüsteemide turvameetmete süsteem ISKE," n.d.; IsecT Ltd., n.d.; ISO/IEC, 2013; IT Governance Ltd, 2015; Kuligowski, 2009)

4.3.3 Interview analysis

The variety of standards, that could be used in a State level is not the question. The problem is when the Member State is not using any, then it is not possible to tell if it is moving in a right direction or if its' security work is consistent.

Specialists brought out the ISKE as a standard used by Estonia regarding the information security. The official audits are still in progress, but as the specialists see, ISKE measures are suitable for assuring the minimum-security requirements. The audit is completed for EURODAC system and the results showed that ISKE is suitable and covers all the requirements set for the systems' security.

On the other hand, it is hard to see, what other Member States are using and if those standards or other security methods are suitable, this is hindering cooperation. In addition to the cooperation there cannot be a certainty of the security of the other Member States' systems if the security measures are not clearly stated. The specialists see the similar grounds in securing the systems as a good solution to bring the level of overall security higher. The problem, the specialists brought out for creating the standardised approach to the systems security is the overregulation There are many regulations already in place, creating new might cause problems with existing inner state and capability of developing the systems according to the new regulations. The new regulation setting the specific requirements for security would be micromanaging by the EU Commission and therefore the Member States are not able to develop according to their better knowledge. Overall requirements shall be acceptable and feasible for all the Member States therefore, EU Commission cannot require high level security if some Member States are not able to comply with them, on the other hand, some Member States are capable for more, and because of the requirement they cannot develop higher level security for the IS.

4.3.4 Conclusions

NIS directives' request for using the internationally accepted security standards would help to make the security evaluation clearer, but none of the interviewees brought out specific preference and need for all the Member States to follow the same standard.

The interviewees would like to have a best practice example which shall be followed, but it should not be official standard, to avoid the growing bureaucracy. They see the example as guideline and minimum requirements, but it should not be the standard, that shall be followed line by line. The guideline shall be flexible and mandatory only for the less capable parties. More capable Member States can design their methods, that are more than set on the minimum level.

5 Conclusions

5.1 Summary of findings

The case study research was carried out to find the necessity for the unified security standard in EU, to secure the large-scale information systems, which have the subsystems in Member States. The information for the research is collected form the EU regulations and interviews. The information collected is analysed using the Thematic analysis method using five themes to answer the research questions. Findings are brought out in the paper.

The first question answered during the research was: "How the system requirements are managed?" The answer is brought out in the first sub-chapter of the analysis which main findings are that there are great amount of bureaucracy in the management of the systems, which in some amount is necessary to operate systems as large as IS used as a case. The decision making goes through multiple levels of authorities and therefore the process is slow. The cooperation is mostly necessity based or covered with the requirements of the regulations, but the knowledge exchange is still weak.

The second question answered was: "How effective are the current regulations, how many of those are mandatory and how is the implementation by Member States monitored?" The answer is in the second subsection of the analysis. The main findings were that the security requirements are comprehensive and give some amount of freedom to choose exact methods, but on the other hand they are bureaucratic and cause the administrative burden to the Member States. The data exchange process is detailed and well regulated by interface control document, on the other hand despite the detailed requirements some problems have arisen and bureaucracy question has been under discussion.

The main question of the research was: "Whether the EU needs a unified standard on ensuring information security of large-scale information systems?" The answer is found in the third subsection of the analysis which states that accepting already existing internationally accepted standard is preferable and gives a better overview of the security measures used, but unified standard is not necessary because of the fear of bureaucracy accompanying the standard. Interviewees would prefer the guidelines that would help to set the main framework for their IS security, but which is not mandatory to use if the minimum requirements are fulfilled.

The hypothesis set for the research: “Standardized approach is necessary to gain the equally high level of security for the EU large-scale information systems.” is proved partially. As the analysis brought out, the unified standard is not necessary, but guidelines and examples that should be mandatory to gain the minimum acceptable level should exist. Therefore, the standardisation of the minimum level is good way to give a viewpoint to the Member States what will be expected from them. Through the cooperation and knowledge sharing, overall level of security can be raised by implementing those measures and thus NIS directive expectations can be reached.

5.2 Suggestions

Based on the analysis the author suggests that at first the national information security measures shall be documented and their compatibility with other Member States standards analysed to be able to make implications about the overall systems’ security.

The second suggestion is that the guideline and minimum requirements shall be worked out on the level of EU-LISA, based on the EU Commission regulations. The responsibility of the management of the guideline shall be stayed on the EU-LISA level and excluding the EU Commission to ensure the flexibility and cooperation and to let the Member States discuss security related topics openly. The regulation granting role shall stay on the EU Commission, but they should not take part of the management work.

Suggestion three covers the reports, regulations and other paperwork, that should be modernised and the decision-making level should be modernised by following the principle of subsidiarity.

The fourth suggestion is that the security of the other communication methods, for example alternative communication channels, should be considered since it could allow opening an attack vector for unauthorized party to gain access to information once primary information systems are rendered non-operational.

5.3 Relation to existing evidence

Research conducted by RAND corporation, whose analyse includes also the same regulations, as in this paper. Both authors got to the result: even though there are many regulations, policies, and directives – those might not improve the overall security of the systems and instead can slow down the progress in IT. Change is needed in forms of less regulations, updated standards and more open communication & information sharing among States specialists. The societal expectations have grown and the technologies have evolved, therefore the existing systems and their regulations are getting outdated.

Some of the RAND corporations' suggestions have been solved already, by the regulations, that were under the discussion during their analysis,

5.4 Limitations

For this research only the public information is used, therefore there are shortcomings or the research is not going as deep as it could go if all the technical information that is classified could be used, but the main questions, that could not get the answers from the documents and reports were answered by the three specialists.

The information gained through interviews, was the view of officials of one Member State, therefore it cannot be extended as an opinion of all representatives of Member States. The main limitations are following:

- Access to the information was limited, because most of the information is classified, because it is about the technical aspects of the systems and therefore has a great offensive value.

- Access to the other Member States officials is limited, mainly because of the essence of the authorities, that are responsible for systems used as a case study. It is challenging at times as a student to get audience with officials.

5.5 Future work

Future work is about covering the shortcomings that affected the accuracy of this paper. The main things that should be done are getting the access to the classified information, which helps to analyse deeper and help to develop the minimum requirements needed to

ensure the equally high level of security. The experience collection in this paper was one-sided and to get the accurate view of the situation in EU, the other authorities shall be interviewed and their experience recorded.

Based on all information it is possible to create the strategic guidelines that can be applied all over the EU.

References

[1] Alonso Blas, D. (2010). Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom. *ERA Forum, 11*(2), 233–250. https://doi.org/10.1007/s12027-010-0158-8

[2] Armoni, A. (2002). Data Security Management in Distributed Computer Systems. *The International Journal Of Science & Technoledge*. Retrieved from http://www.inform.nu/Articles/Vol5/v5n1p019-027.pdf

[3] Boehm, F. (2012). *Information sharing and data protection in the area of freedom, security and justice: towards harmonised data protection principles for information exchange at EU-level*. Berlin ; Heidelberg: Springer.

[4] Booth, G. M. (1976). Distributed information systems (p. 789). ACM Press. https://doi.org/10.1145/1499799.1499907

[5] British Standard Institution. (2013). ISO27002:2013 -Information technology Security techniques Code of practice for information security controls.

[6] Bundesamt für Sicherheit in der Informationstechnik. (2007). IT Security Guidelines. IT-Grundschutz in brief. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/IT-sec-guidelines_pdf.pdf?__blob=publicationFile&v=1

[7] Bundesamt für Sicherheit in der Informationstechnik. (2016). *IT-Grundschutz catalogues. 15th version*. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/GSK_15_EL_EN_Draft.pdf?__blob=publicationFile&v=2

[8] COMMISSION OF THE EUROPEAN COMMUNITIES. (2004). *COMMISSION STAFF WORKING PAPER First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*. Brussels.

[9] Data Protection: unauthorized access to personal data in the systems that the National Police is responsible for data for. (n.d.). Retrieved March 6, 2017, from https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/vedroerende-uvedkommendes-adgang-til-personoplysninger-rigspolitiets-jnr-2013-079-76/

[10] Eesti Standardikeskus. (2017). EVS-EN ISO/IEC 27001:2017. Retrieved April 1, 2017, from https://www.evs.ee/Checkout/tabid/36/screen/subscription/orderid/22c103d2-53a8-4ad2-a015-006314601009/Default.aspx

[11] European Commission. (2003). Commission communication regarding the implementation of Council Regulation (EC) No 2725/2000 “Eurodac.”

[12] European Commission. (2015). COMMISSION IMPLEMENTING DECISION (EU) 2015/219 of 29 January 2015 replacing the Annex to Implementing Decision 2013/115/EU on the Sirene Manual and other implementing measures for the second generation Schengen Information System (SIS II). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D0219&qid=1493561467835&from=ET

[13] European Commission. (2017). COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D0046&from=EN

[14] European Commission, & Directorate-General for Migration and Home Affairs. (2015). Europe without borders: the Schengen area. Luxembourg: Publications Office. Retrieved from http://bookshop.europa.eu/uri?target=EUB:NOTICE:DR0215167:EN:HTML

[15] European Council. (2000). NÕUKOGU MÄÄRUS (EÜ) nr 2725/2000, 11. detsember 2000, mis käsitleb sõrmejälgede võrdlemise Eurodac-süsteemi kehtestamist Dublini konventsiooni tõhusa kohaldamise eesmärgil.

[16] European Parliament, Council of the European Union. (2006). 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). European Parliament, Council of the European Union. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1987&qid=1486316285211&from=EN

[17] European Parliament, Council of the European Union. (2011). 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. European Parliament, Council of the European Union. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R1077&from=EN

[18] European Parliament, Council of the European Union. (2013). EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) nr 603/2013, 26. juuni 2013, millega luuakse sõrmejälgede võrdlemise Eurodac-süsteem määruse (EL) nr 604/2013 (millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest) tõhusaks kohaldamiseks ning mis käsitleb liikmesriikide õiguskaitseasutuste ja Europoli taotlusi sõrmejälgede andmete võrdlemiseks Eurodac-süsteemi andmetega õiguskaitse eesmärgil ning millega muudetakse määrust (EL) nr 1077/2011, millega asutatakse Euroopa amet vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimiseks (uuesti sõnastatud). Retrieved from http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32013R0603&qid=1490452425573&from=EN

[19] European Parliament, Council of the European Union. (2016a). DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1493557208228&from=ET

[20] European Parliament, Council of the European Union. (2016b). EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. Retrieved from http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016L0680&qid=1476170475962&from=ET

[21] European Parliament, Council of the European Union. (2016c). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data

Protection Regulation). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1491325269262&from=EN

[22] Gudmundsson, A., Boer, H., & Corso, M. (2004). The implementation process of standardisation. *Journal of Manufacturing Technology Management*, *15*(4), 335–342. https://doi.org/10.1108/17410380410535035

[23] Infosüsteemide turvameetmete süsteem ISKE. (n.d.). Retrieved March 7, 2017, from https://www.ria.ee/ee/iske.html

[24] IsecT Ltd. (n.d.). ISO/IEC 27001 certification standard. Retrieved March 8, 2017, from http://www.iso27001security.com/html/27001.html

[25] ISO/IEC. (2013). ISO/IEC 27002:2013(en), Information technology — Security techniques — Code of practice for information security controls. Retrieved March 8, 2017, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

[26] IT Governance Ltd. (2015). INFORMATION SECURITY & ISO 27001 AN INTRODUCTION. Retrieved March 8, 2017, from https://www.itgovernance.co.uk/download/Infosec-and-ISO27001v4-uk.pdf

[27] Kirchgaessner, S. (2016). Anis Amri, Berlin attack suspect, shot dead by police in Milan. Rome, Italy. Retrieved from https://www.theguardian.com/world/2016/dec/23/anis-amri-berlin-attack-suspect-shot-dead-milan

[28] Kuligowski, C. (2009). *COMPARISON OF IT SECURITY STANDARDS*. Retrieved from http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf

[29] Li, W., Xie, Y. F., Gui, W. H., & Ding, S. X. (2010). Decentralised fault detection of large-scale systems with limited network communications. *IET Control Theory & Applications*, *4*(9), 1867–1876. https://doi.org/10.1049/iet-cta.2008.0604

[30] Marquenie, T. (2017). The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework. *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2017.03.009

[31] National Research Council. (2000). *Making IT Better: Expanding Information Technology Research to Meet Society's Needs.* Washington: National Academies Press. Retrieved from http://public.eblib.com/choice/publicfullrecord.aspx?p=3375508

[32] Ritchie, J., Lewis, J., McNaughton Nicholls, C., & Ormston, R. (Eds.). (2014). *Qualitative research practice: a guide for social science students and researchers* (Second edition). Los Angeles: Sage.

[33] Robinson, N., & Gaspers, J. (2014). *Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies*.

[34] Rull, A., Täks, E., & Norta, A. (2014). Towards Software-Agent Enhanced Privacy Protection. In T. Kerikmäe (Ed.), *Regulating eTechnologies in the European Union* (pp. 73–94). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-08117-5_5

[35] RUNESON, P., HOST, M., RAINER, A., & REGNELL, B. (2012). *CASE STUDY RESEARCH IN SOFTWARE ENGINEERING*.

[36] Secretariat of the Eurodac Supervision Coordination Group. (2009). *Eurodac Supervision Coordination Group Second Inspection Report*. Brussels: European Data Protection Supervisor. Retrieved from https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Eurodac/09-06-24_Eurodac_report2_EN.pdf

[37] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (2008). 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). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008R0767&qid=1488206026383&from=EN

[38] Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study: Qualitative descriptive study. *Nursing & Health Sciences*, *15*(3), 398–405. https://doi.org/10.1111/nhs.12048

[39] Vithanage, D. K. A., & Wijayanayake, W. M. J. I. (2007). Insight to the large scale Information Systems implementation in Sri Lanka. In *2007 International Conference on Industrial and Information Systems* (pp. 33–40). https://doi.org/10.1109/ICIINFS.2007.4579144

[40] Wellens, P. (2013). *TESTA NG*. Retrieved from https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/pieter-wellens-digit-the-stesta-infrastructure.pdf

[41] What is standardization? definition and meaning. (n.d.). Retrieved May 6, 2017, from http://www.businessdictionary.com/definition/standardization.html

[42] Williams, M. (2000). Interpretivism and Generalisation. *Sociology*, *34*(2), 209–224. https://doi.org/10.1177/S0038038500000146

[43] Yin, R. K. (2014). *Case Study Research: Design and Methods 5th Edition*. SAGE Publications.

[44] Zampaglione, L. (2017). Interview with Security Officer of the EU-LISA.

[45] Zheng, Y., Li, S., & Li, N. (2011). Distributed model predictive control over network information exchange for large-scale systems. *Control Engineering Practice*, *19*(7), 757–769. https://doi.org/10.1016/j.conengprac.2011.04.003