Understanding the threat landscape in e-government infrastructure for business enterprises

Harikrishnan Pushpakumar

Delft University of Technology
September 22, 2015

TU Delft Delft University of Technology

Understanding the threat landscape in e-government infrastructure for business enterprises

Master of Science Thesis

Committee Chair:
Prof.dr. M.J.G. (Michel) van Eeten

Supervisors:
Dr. Ir. W. Pieters
Dr. Ir. D. Hadziosmanovic
Dr.ing. A.J. (Bram) Klievink
T.Koopmanschap MA (Logius)

Author:
Harikrishnan Pushpakumar
Student No: 4300866

DELFT UNIVERSITY OF TECHNOLOGY

Faculty of
Technology, Policy and Management (TBM)
Management of Technology

22nd September 2015
Delft

Thanks Mom, Dad, & Sush.
Your unparalleled support has been the greatest inspiration for me.

Executive Summary

Cyber threats are becoming more sophisticated and varied. The range of possible attacks that organizations face is higher than in the past. Analysis shows that the number of cyber incidents involving government agencies has increased by 35 percent between 2010 and 2013 (Frates & Devine, 2014). E-government is a potential target to attacks of various kinds from a range of adversaries. The adversaries can be disgruntled current or former employees, hackers, script kiddies, virus writers, criminal groups, corporate espionage groups, terrorists, foreign intelligence agencies, state backed actors, and various other actors (Dutta & Mccrohan, 2002). The rising number of cyber threats and the increasing complexity of e-government implementations call for enhanced security of e-government infrastructures. The preparedness of organizations to future cyberattacks depends on the awareness of the organizations about their cyber threat landscape. The threat landscape of an organization shows the range of threats that the organization faces from a security perspective. We define a threat landscape as the characteristics (attributes), the likely threat actions (methods), and objectives of the different types of threat agents who may act against the assets of an organization. In this research we focus on understanding the threat landscape of e-government infrastructure for business enterprises. Contemporary research shows a gap in understanding the threat landscape of e-government infrastructures. A systematic methodology for understanding the threat landscape of e-government infrastructures is also lacking. We argue that a threat assessment methodology can be used to understand the threat landscape of e-government infrastructure for businesses. Based on this argument we formulated our main research question, ***"How can a threat assessment methodology be used to understand the threat landscape of e-government infrastructure for businesses?"*** To answer the main research question we formulate four sub-questions which are answered in the various phases of the Action Design Research (ADR) model by Sein et al. (2011).

In the *Problem Formulation* phase, we introduce the research problem and frame the research questions. We then explain the concept of e-government infrastructure for businesses and describe Digipoort - a representative case of e-government infrastructure for businesses used in this research, owned by the Dutch government and managed by Logius. Our analysis of the state of the art in threat assessment methodologies shows that the Threat Agent Risk Assessment (TARA) methodology developed by Intel is suitable for understanding the threat landscape of organizations. However applying the TARA methodology to e-government infrastructure for businesses is only possible by overcoming the limitations of the Threat Agent Library (TAL) and the Methods & Objectives Library (MOL) associated with it. In the *Build, Intervention and Evaluation (BIE)* phase we address the limitations of the TARA methodology by tailoring the TAL and MOL for e-government infrastructure for businesses. We use knowledge from information security literature and cyber security experts in the public sector to perform this. The outputs of the *BIE* phase are the tailored TAL and MOL for e-government infrastructure for businesses. In the *Reflection and Learning* phase, we apply the tailored TAL and MOL using TARA methodology to the Public Key Infrastructure (or *Key Management System*) of Digipoort PI. We use knowledge from technical documents in Logius, information security literature and experts at Logius to perform this. The results of the application help us in understanding the threat landscape of the PKI of Digipoort PI, and reflect and learn about the tailored TAL and MOL we designed. We conclude

the research in the *Formalization of Learning* phase where we draw the main conclusions and reflect on the learning from the research.

This research contributes to the field of Information Security by providing a tailored library of threat agents for the e-government domain. We also summarize the methods and objectives of the threat agents in the corresponding library of methods and objectives. Organizations like Logius wanting to enhance their understanding of the threat landscape of e-government infrastructure for businesses can use these libraries as a starting point for threat assessment. Furthermore, this research also provides opportunities for future research in this area as the libraries can be tailored for applying to other infrastructures in the e-government domain or new domains itself.

Acknowledgments

Cyber security as an area of research was not in my radar when I joined this program two years back. The increasing relevance of cyber security in this connected world of technology and a very inspiring course from Prof. dr. ir. J. (Jan) van den Berg on Cyber Security Essentials, inspired me to walk down this increasingly explored area of socio-technical research in cyber security. I have learned so much in the past 6-7 months that no amount of theoretical knowledge could have prepared me for. However, this journey would not have been easy without the guidance and support of many people.

I would like to thank my committee chair, Prof.dr. M.J.G. (Michel) van Eeten for his guidance and support in the research. My first supervisors, Dr.ir. W. Pieters (Wolter) and Dr.ir. Dina Hadžiosmanović have been incredible sources of inspiration and support throughout the thesis. I would like to thank them for giving me the opportunity to work in the TREsPASS project. Their critical feedback enabled me to take my own decisions during the research. I would especially like to thank Dina for the regular consultations and words of encouragement. I admire her patience in reviewing and correcting the incredible number of draft reports I produced. I would also like to thank my second supervisor, Dr.ing. A.J. (Bram) Klievink for his willful support and feedback during the thesis.

This thesis would not have been possible without the support of my colleagues at Logius. I would like to thank Tim Koopmanschap for his constant support and constructive feedback as my external supervisor. I express my sincere gratitude to Victor Toom for his timely support and technical inputs. I would also like to thank all the interviewees who found time to share their valuable opinions. There are many others at Logius I want to thank - Eric, Rochelle, Laurens, Baldwin, Koen, Kim, Michel, Mike, Wouter, Roeland, Curtly, Anna, Peter, and Tanaquil, you have been incredibly helpful.

I want to thank all my friends for supporting me with their encouraging words and feedback during the thesis. The discussions and peer reviews in the TREsPASS peer group - Rick, Katrien, Dimitris, and Yiwen, have been really helpful. Nitish and Istvan, I thoroughly enjoyed all our discussions about cyber security and other cool subjects. I also thank Abhilash for his patience in proof reading a 200 page report.

Finally, I want to thank my family who has been incredibly supportive throughout my studies. Without your unconditional love and support, I would not have dared to venture out of my comfort zone and expand my horizons.

-Harikrishnan Pushpakumar
Delft, 4th September 2015

Contents

List of Figures

List of Tables

List of Acronyms

BIR	Baseline Informatiebeveiliging Rijksdienst
BIE	Build, Intervention, Evaluation
CA	Certificate Authority
CEL	Common Exposures Library
CER	Certificate
CRL	Certification Revocation List
CSP	Certificate Service Provider
CSR	Certificate Signing Request
DNB	De Nederlandsche bank
DOS	Denial of Service
DDOS	Distributed Denial of Service
FAIR	Factor Analysis for Information Risk
FTP	File Transfer Protocol
GTM	General Threat Matrix
KD	Keteninformatiediensten
MinBZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
MOL	Methods & Objectives Library
MS	Managed Services
NVWA	Nederlandse Voedsel- en Warenautoriteit
OCSP	Online Certificate Status Protocol
OTA	Operational Threat Assessment
OTP	Overheidstransactiepoort
PEM	Privacy Enhanced Mail
PI	Process Infrastructure
PKI	Public Key Infrastructure
POP	Post Office Protocol
PoR	Program of Requirements
SBR	Standard Business Reporting
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TAL	Threat Agent Library
TAME	Threat Assessment Model for Electronic Payment Systems
TARA	Threat Agent Risk Assessment
TLS	Transport Layer Security
TSA	Cyber Threat Susceptibility Assessment
TTP	Trusted Third Party
UDDI	Universal Description, Discovery and Integration
UML	Unified Modeling Language
UWV	Uitvoeringsorgaan Werknemers Verzekeringen
WSDL	Web Service Description Language
WUS	Web Services, UDDI and SOAP
XBRL	eXtensible Business Reporting Language
XML	Extensible Markup Language

INTRODUCTION

1. Background

Cyberattacks on organizations are increasing in both frequency and severity (Symantec Corporation, 2014). The range of attacks that organizations face is higher than in the past. There is an increase in the volume and variety of attacks owing to the financially and criminally motivated threat agents' desire to obtain personal or confidential information and disrupt services (Choo, 2011b). Organizations today rely heavily on cyberspace to reach out to new and existing customers across geographical and demographical dissimilarities. With the increased dependence of organizations on cyberspace, there has been increase in the threats too. Though there has been increased awareness, technology capabilities, market and vendor focus on cyber security, the ever evolving cyber risk and attacks makes it necessary to keep the threat landscape of the organizations updated (Bharti, 2011).

Various evidences suggest that cyberattacks on governments are on the rise. According to a report from the Government Accountability of US, the number of cyber incidents involving government agencies has increased by 35 percent between 2010 and 2013 (Frates & Devine, 2014). The attack on prominent Estonian government websites in 2007 had the alleged involvement of Russian government agencies (IAR, 2014). State sponsored attacks like spying leads to data loss and possible endangering of lives of employees. Recently, hackers believed to be sponsored by the Chinese government broke into US government computers, possibly compromising the data of 4 million current and former federal employees (Spetalnick & Brunnstrom, 2015). The Canadian government faced a highly sophisticated Chinese state sponsored attack, which forced them to revamp their information technology infrastructure (Vieira & King, 2014). Hackers recently broke into several German government websites, including the German chancellor Angela Merkel's pages for political reasons (Wagstyl, 2015). During the 2009 protests over Iranian election results, activists enlisted social media like Twitter to spread their message resulting in a massive Denial of Service (DoS) attacks against government web servers (Stiennon, 2010). Recent studies by the National Cyber Security Centre (NCSC) shows that the number of cyberattacks on Dutch government websites and systems has doubled over the past two years (DutchNews.nl, 2015a). A research by Symantec also shows that Netherlands is the number one country in Europe and fourth in the world in being targeted by cyber criminals (DutchNews.nl, 2015b). These examples show that cyber threats are an increasing concern for e-governments in general and especially for e-government of the Netherlands.

E-government is an amalgam of heterogeneous information systems in which a high volume of information exchange happens through the interaction of government agencies with public and private sector organizations. Such intricate interdependence can only be supported by secure information infrastructures (Joshi et al., 2001). Choo (2011) and Bharti (2011) mentions that a clear understanding of the threat landscape is necessary to mitigate the cyber risks to organizations and its infrastructures. This research therefore focuses on understanding the threat landscape of e-government infrastructures. A threat landscape consists of the information needed to understand the agents who may act against our asset (The Open Group, 2010). In practical terms, a threat landscape is mainly a structure of classification of threats, the threat actions, and their characteristics. ENISA reports threat landscape as the developments in cyber threats, threat agents and trends. Identification of threat agents is an

important part of the process (Marinos, 2013). There is however no clear definition of a threat landscape or what it includes. In this research, threat landscape is defined as the characteristics (attributes), the likely threat actions (methods), and objectives of the different types of threat agents who may act against the assets of an organization. We discuss in detail the conceptualization of a threat landscape from literature in Chapter 5 of this report.

1.1. Motivation for Research

E-government is defined as the use of information and communication technologies to enable the daily administrative activities of governments. The potential of e-government to provide services that are designed for the citizen's needs, and increase efficiency of the working government are well understood (Moon, 2002). E-government provides many advantages like improved efficiency and effectiveness of agency activities and programs, which leads to cost savings (Carter & Bélanger, 2005). At the same time, security is one among the primary concerns for e-government. Cyber intrusions could lead to the disruption of e-government services (Halchin, 2004). E-government is a potential target to attacks of various kinds from a range of adversaries as discussed earlier. The adversaries can be disgruntled current or former employees, hackers, script kiddies, virus writers, criminal groups, corporate espionage groups, terrorists, foreign intelligence agencies, state backed actors, and various other actors (Dutta & Mccrohan, 2002). We presented many examples of attacks on e-government infrastructures earlier in the chapter. The incidents show the variety of threat agents with varied capabilities and intentions that can act against e-government infrastructures. This makes it necessary to understand and keep up to date the threat landscape of e-government infrastructures. However, literature shows that there are gaps in understanding the threat landscape of e-government infrastructures.

Choo (2014) mentions that in order to understand the threat landscape due to cyber threats, it is important for governments to understand the interplay of threat actor(s), the international and domestic environment, and the target(s) of attacks. Choo (2011b) provides a snapshot of the contemporary cyber threat landscape by mainly focusing on financially motivated criminals. His work shows an analysis of the risk areas for organizations, however without any differentiation between the public and private sectors. Choo (2011a) performed a survey of the threat landscape of the Australian financial and insurance industry by examining the top four risk areas reported by survey participants, mainly malware, phishing, insider abuse, and theft or loss of proprietary or confidential information. Marinos & Sfakianakis (2012); Marinos (2013, 2014) published by ENISA annually, shows the top threats, trends observed and threat agents for organizations, based on the analysis of published reports on threat intelligence from private and public organizations collected using Open Source Intelligence (OSINT) methods. The National Cyber Security Centre (NCSC) of Netherlands publishes the Cyber Security Assessment Netherlands (CSAN) annually to offer insights into developments, interests, threats and resilience in the field of cyber security for public and private organizations in the Netherlands. The NCSC gathers information about the cyber threat landscape from publicly accessible sources, surveys, information from the vital sectors and collaboration with many government and non-government organizations (NCSC, 2014). In addition various consulting and security organizations like Verizon, Symantec regularly releases threat landscape reports for selected industries like healthcare, retail and hospitality, financial services etc (Symantec, 2014; Verizon, 2015a). In the literatures discussed above we

see many artifacts on cyber threat landscape information, both generic as well as for specific industries, published by researchers, governmental organizations and consultancies. The threat landscapes shown in these reports are mainly the results of surveys of security personnel and analysis of threat intelligence data collected over the years from various publicly available sources. We realize two main gaps from this.

1) An exclusive focus on the analysis of the threat landscape in e-government infrastructures is lacking.
2) A systematic methodology for studying the threat landscape of e-government infrastructures is lacking.

Based on the gaps identified, our problem statement is that "understanding the threat landscape of e-government infrastructures is currently difficult because a systematic methodology for studying the threat landscape of e-government infrastructures is lacking". To address the problem, we argue that a threat assessment methodology can be used to systematically study the threat landscape of e-government infrastructures. Based on this argument, we will explore and adapt a suitable threat assessment methodology for understanding the threat landscape of e-government infrastructures. In the following chapter we set the scope, objective, and research questions of the research. We also describe the research methodology we will be using to address the research questions.

2. Research Objectives & Methodology

In Chapter 1 we defined a threat landscape and also discussed the gap in understanding the threat landscape of e-government infrastructures. Keeping these in mind, in this chapter we describe the scope and objective of the research, the research questions and the research methodology we use to achieve the objective of this research.

2.1. Scope & Objective

Scope

According to the Factor Analysis for Information Risk (FAIR) taxonomy, a threat is defined as:
"Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures." (The Open Group, 2009)

In this research, we define *threat* in terms of human actors that can cause harm to the organization and its assets. This can include malicious and non-malicious human actors. Errors or failures due to the actions of the human actors are also considered. Mechanical errors, system errors due to natural causes, acts of God (weather, geological events, etc.) are excluded from the scope of this analysis. The exclusive focus on threat agents reduces visibility about the vulnerabilities, however it helps the organizations develop a more coherent picture of the threat space and priorities of remediation (Casey et al., 2010). The focus on threat agents is therefore better suited for studying the threat landscape of an infrastructure and hence for this research.

E-government as a domain is vast with different types of services being provided by the government to different types of stakeholders. The stakeholders can be citizens, businesses, employees of the government or other government agencies (Carter & Bélanger, 2005). However, the scope of our research is limited to the e-government infrastructure for businesses. More specifically, we focus only on the Government to Business (G2B) and Business to Government (B2G) interactions. In the former businesses are the regulated economic sector using services like eCustoms, and in the latter government acts as the customer using services like eProcurement (Henriksen et al., 2008). Bekkers (2003) refer to two types of services related to this - *Transaction Services* and *Data Transfer Services. Transaction Services* refer to the electronic intake and handling of requests and applications of benefits and obligations like digital tax assessments, the render of permits, licenses and subsidies. *Data Transfer Services* refer to the exchange and sharing of basic and standard information between governments and businesses (Bekkers, 2003). In the Netherlands, these services are particularly well developed and intricate as made evident by their high ranking in the 2014 United Nations E-government survey (UN, 2014).

Case Selection

This research is performed in association with Logius, under the Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (MinBZK). A very important e-government infrastructure for businesses owned by the Dutch government and managed by Logius is Digipoort. Digipoort provides the communication

infrastructure for exchange of digital information between businesses and government authorities. The two types of Digipoort – Digipoort OTP and Digipoort PI play a major role in the transfer of different types of messages like customs, and tax information from businesses to government authorities. Digipoort OTP and Digipoort PI are two functionally similar but technically separated infrastructures maintained by Logius.

Two factors make Digipoort suitable for our research. First, Digipoort is widely used by businesses and governments in the Netherlands for exchange of digital information. Since its inception in 2004 with 40 companies involved in the pilot, Digipoort has grown to serve more than 700 participating companies (EPractice, 2012). Around 71.5 million messages by more than 700 companies were sent through Digipoort (Digipoort OTP and PI) in 2012 (Logius, 2015i). This shows the pervasiveness of Digipoort as an e-government service. Second, the continuous availability of Digipoort is critical to many services of the Dutch government. The unavailability of Digipoort to the Douane (customs department) will affect the entire logistics chain of goods import to the Netherlands and will lead to considerable cost escalation (EPractice, 2012; Logius, 2015i). This shows the importance of securing Digipoort from any internal or external attacks. Based on the pervasiveness of its use and the criticality of its service, we consider Digipoort as a representative case for e-government infrastructure for businesses in this research.

Objective

With the scope limited to e-government infrastructure for businesses, the main objective of the research is to make the understanding of threat landscape of e-government infrastructure for businesses possible. Based on our earlier argument, in order to understand the threat landscape of e-government infrastructure for businesses, it is necessary to understand the existing threat assessment methodologies, adapt and use a methodology suitable for e-government infrastructure for businesses.

2.2. Research Questions

To achieve the research objective mentioned above we formulate the main research question in the following manner.

"How can a threat assessment methodology be used to understand the threat landscape of e-government infrastructure for businesses?"

We expect that the output of the main research question will give us an adapted methodology for understanding the threat landscape of e-government infrastructure for businesses. We devise four sub-questions in order to systematically answer the main research question.

SQ 1: What are e-government infrastructures for businesses?

SQ 2: What is the state of the art in threat assessment methodologies for e-government infrastructures?

SQ 3: How can a threat assessment methodology be adapted for e-government infrastructure for businesses?

SQ 4: What are the results of applying the adapted threat assessment methodology in a practical case study?

2.3. Research Methodology

In this section we explain the research methodology used to answer the research sub-questions and thereby the main research question. To structure this research we use the Action Design Research (ADR) model developed by Sein et al. (2011). ADR recognizes that the design artifact emerges from interaction with the organizational context while also learning about the class of problems. This research aims to adapt an existing threat assessment methodology for e-government infrastructure for businesses. This process happens in close interaction with the organizational context of Digipoort. Unlike the stage-gate models of design, ADR also recognizes that evaluation is not a separate stage that follows building. Decisions about designing, shaping and reshaping the artifact are interwoven with ongoing evaluation (Sein et al., 2011). This is also true in our case as we do not have a separate stage for evaluation, but the design was continuously evaluated using knowledge from literature. Figure 1 shows the various stages of the research and how they align with the ADR design model.

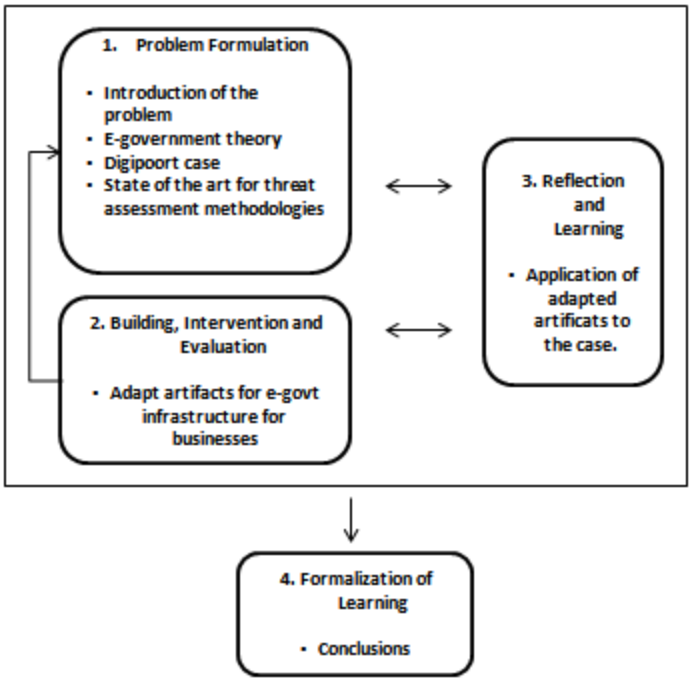

Figure 1: Research Methodology based on ADR, adopted from (Sein et al., 2011)

Under the *Problem Formulation* we introduce the problem and discuss e-government and the specific case of Digipoort. We also discuss the state of the art in threat assessment methodologies from which a suitable threat assessment methodology is selected for adaptation. This phase results in the structuring of the problem, identifying solution possibilities, and guiding the design (Sein et al., 2011). The *Building, Intervention and Evaluation (BIE)* discuss the adaptation of the threat assessment methodology for e-government infrastructure for businesses based on the results of the previous stage. The *Reflection and Learning* stage involves conscious reflection on the problem framing, the theories chosen, and the

artifact designed to ensure that contributions to knowledge are identified (Sein et al., 2011). In this stage we apply the adapted methodology to an asset of Digipoort and reflect on the findings. Further, in the *Formalization of Learning* we discuss the conclusions made from the adaptation of the threat assessment methodology and the outcomes that can be generalized from the research. The four sub-questions are answered in the various stages of research as explained below and summarized in Table 1.

Problem Formulation

- ***Introduction***

The introduction stage describes the problem perceived with respect to the understanding of the threat landscape of e-government infrastructures. The increasing cyber incidents on e-government infrastructures show the necessity for studying their threat landscapes. However, existing literature and studies do not focus explicitly on understanding the threat landscape of e-government infrastructures. We also perceived the lack of a suitable methodology for studying the threat landscape of e-government infrastructures, based on which we argued that an existing threat assessment methodology could be adapted for this purpose. We limited the scope of our research to e-government infrastructure for businesses, based on which we arrived at the main research question, *"How can a threat assessment methodology be used to understand the threat landscape of e-government infrastructure for businesses?",* and four sub-questions which are answered in the various phases of the ADR model.

- ***Exploration***

We will answer the first sub-question in this part. Chapter 3 will explain the concept of e-government infrastructure in general and reiterate why government organizations need to understand their threat landscapes. We selected Digipoort as a case of e-government infrastructure for businesses based on its criticality and its pervasive use by businesses and governments in the Netherlands. Chapter 4 describes the technology and services of Digipoort, and the actors involved in the working of e-government infrastructure for businesses. We distinguish between the two services of Digipoort – Digipoort OTP and Digipoort PI, and describe in detail their infrastructure and services. We also develop use case models of Digipoort OTP to understand the interaction of Digipoort with the actors involved. We use desk research to gather the knowledge required to answer this sub-question. We will use academic literature (books, journals etc) to learn about e-government, and its general architecture. In order to study Digipoort, its technology and services, we use internal technical documents about Digipoort provided by Logius, and the websites of Logius. The results from this sub-question will be used in adapting the threat assessment methodology for e-government infrastructure for businesses, which will be handled in the third sub-question.

- ***State of the art***

We will answer the second sub-question in Chapter 5. SQ 2 will aid us in first understanding the state of the art in threat assessment methodologies and selecting a suitable methodology for understanding the threat landscape. We will also analyze the limitations of the identified methodology in using it for understanding the threat landscape of e-government infrastructure for businesses. In order to answer SQ 2 we will use a desk research method by reviewing academic (books, journals etc.) and non-academic (white papers, technical reports etc.) literature on threat assessment methodologies.

Building, Intervention and Evaluation (BIE)

- ***Design***

We will answer the third sub-question in Chapter 6. SQ 3 deal with the adaptation of the threat assessment methodology for e-government infrastructure for businesses. We use a combination of desk research and interview of security and cyber risk experts in the public sector to answer this question. We will use artifacts from academic (books, journals etc.) and non-academic (white papers, technical reports etc.) literature in information security, cyber security, publically available incident databases et al. for the desk research. Further, we will also use the inputs of security and cyber risk experts in the public sector wherever necessary to fill gaps in the analysis that cannot be filled from the available literature. The output of this sub-question will be an adapted methodology that can be applied on e-government infrastructure for businesses to understand their threat landscape.

Reflection and Learning

- ***Application***

We will answer the fourth sub-question in Chapter 7. SQ 4 deal with the application of the tailored methodology on a practical case of e-government infrastructure for businesses. We apply the methodology on Digipoort PI, the second variant of Digipoort. Digipoort PI as an infrastructure is more complex in application and implementation than Digipoort OTP (discussed in Chapter 3), and therefore could give us more insights in terms of reflection and learning. Moreover, Digipoort OTP is a legacy system and will be replaced by Digipoort PI in the near future. Based on these factors we decided to apply the methodology on Digipoort PI and not on Digipoort OTP. We will use internal technical documents about Digipoort PI provided by Logius to understand the working of Digipoort PI, and will also interview technical experts and information security experts in Digipoort PI at Logius to answer this sub-question.

Formalization of Learning

- ***Conclusion***

In Chapter 8 we discuss the conclusions from the research. We discuss the outputs to the sub-questions and address the main research question. Based on the findings through the ADR process, we try to draw inferences which can be generalized as knowledge gained from the research. We also discuss the main contributions, and limitations of our research.

Table 1: Research Approach

No.	Research Sub-questions	Knowledge Required	Type of Inputs	Research Part
1	What are e-government infrastructures for businesses?	✓ E-government. ✓ General architecture of e-govt. ✓ Digipoort services and use cases.	✓ Literature about e-govt. ✓ Documents about Digipoort from Logius.	Exploration

No.	Research Sub-questions	Knowledge Required	Type of Inputs	Research Part
2	What is the state of the art in threat assessment methodologies for e-government infrastructures?	✓ Threat assessment methodologies.	✓ Literature review of academic and non-academic publications on threat assessment methodologies.	State of the art
3	How can a threat assessment methodology be adapted for e-government infrastructure for businesses?	✓ Threat agents relevant for e-government infrastructures. ✓ Knowledge about characteristics of threat agents. ✓ Expert knowledge to characterize the attributes, methods and objectives of newly identified threat agents.	✓ Knowledge from SQ2. ✓ Past incident data in the public sector. ✓ Interview of experts in security and cyber risk in the public sector.	Design
4	What are the results of applying the adapted threat assessment methodology in a practical case study?	✓ Knowledge about assets and working of Digipoort PI. ✓ Knowledge about architecture and controls of Digipoort PI.	✓ Documents about Digipoort PI from Logius. ✓ Architect and security expert advice from Logius.	Application

In this section we discussed the research methodology used to answer the main research question and the four sub-questions. We also identified the knowledge required for answering each sub-question and the type of research we will be using to obtain this knowledge.

2.4. Scientific Relevance

This research is relevant to the field of information security in two ways. First, in this research we conceptually define a threat landscape. Even though threat landscape as a term is commonly used in information security literature, no clear definition is attributed to it from theory. Through an initial literature analysis we develop a conceptual model for a threat landscape in this research. This is discussed in Chapter 5. Second, we adapt a threat assessment methodology for the domain of e-government infrastructure for businesses. In the *BIE* phase of the research we tailor a library of threat agents and study their attributes, methods and objectives for e-government infrastructure for businesses. To the best of our knowledge, this work can be considered as the primary attempt to tailor a library of threat agents for e-government domain. The library shows a fundamental understanding of various threat agent characteristics and will help researchers in the field of information security by acting as a pre-defined matrix of threat agents relevant for e-government infrastructure for businesses. This reduces the time and effort researchers need to spend in studying multiple literature sources for understanding specific characteristics of each threat agent.

2.5. Societal Relevance

With rising cyber incidents against e-government infrastructures, the development of a methodology that can be used to understand the threat landscape of e-government assets is valuable for governmental organizations. The adapted threat assessment methodology we present can be used by governmental organizations and consultancies to develop the threat landscape of e-government infrastructure for businesses. The library of threat agents we tailor in the *BIE* phase of the research can act as a starting point for threat landscape analysis in general. The library can be updated according to the increasing diversity of cyber threats which makes the artifact even more valuable for organizations wanting to understand their potential threats and vulnerabilities. Organizations can prioritize their critical areas of focus using the threat agent library and apply measures accordingly. This saves both time and resources for organizations.

For Logius, this research will provide a ready to apply library of threat agents that can be used to add value to their existing risk management capabilities. They can use the adapted threat assessment methodology to understand the threat landscape of their e-government infrastructure for businesses. In the *Reflection and Learning* phase of the research we also demonstrate this by performing a minimal implementation of the adapted threat assessment methodology on Digipoort PI. The results from the implementation contribute to the existing knowledge that Logius has about Digipoort, its threat landscape, vulnerabilities and controls. In the future, Logius can also extend the threat agent library to be applied for their many other e-government services provided to stakeholders other than businesses.

2.6. Thesis Structure

In this section we describe the overall structure of the thesis as shown in Figure 2. The report is structured as follows. In Chapter 1 we described the background of the research and motivation for the research. In Chapter 2 we defined the scope and objective of the research in Section 2.1. Based on the objective defined we formulated the main research question as ***"How can a threat assessment methodology be used to understand the threat landscape of e-government infrastructure for businesses?"***, and devised four research sub-questions to systematically answer it. In Section 2.3 we described the research methodology based on the Action Design Research model developed by Sein et al. (2011). Figure 1 shows the various stages of the ADR model and Table 1 summarizes the research approach used for answering the four sub-questions.

In the remaining part of the report, Chapter 3 and Chapter 4 will answer the first sub-question. Chapter 5 concerns the state of the art where the second sub-question will be answered. Chapter 6 concerns the design part of research and the third sub-question. Furthermore, Chapter 7 deals with application part where we will answer the fourth sub-question. Subsequently, in Chapter 8 we summarize the main conclusions from this research.

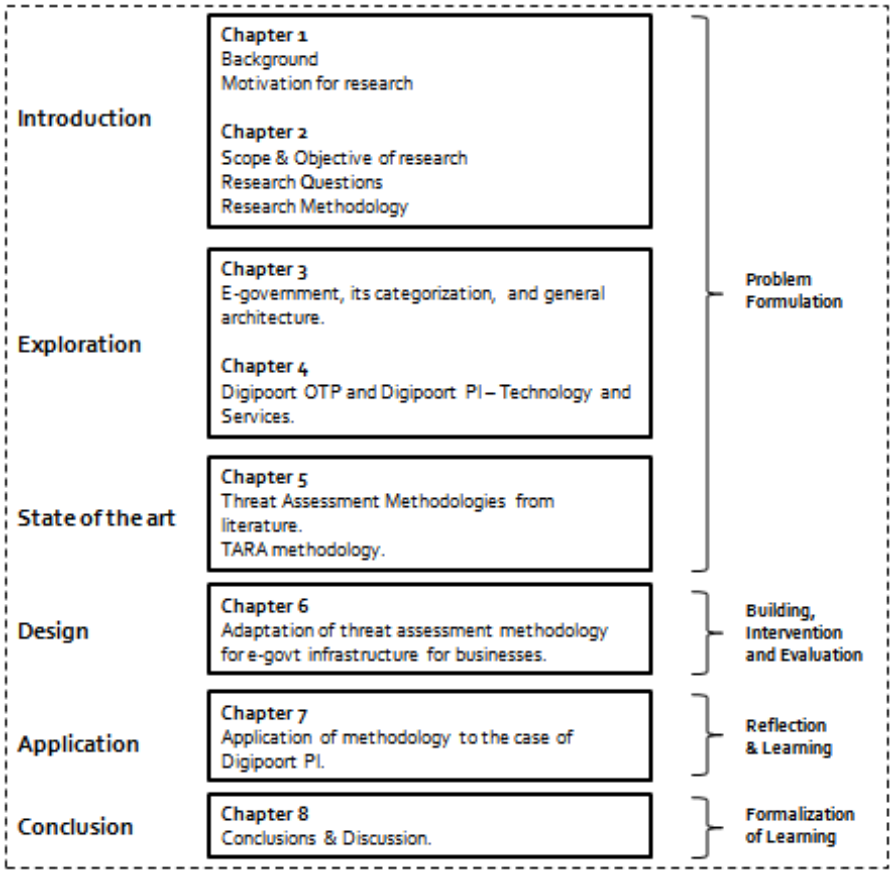

Figure 2: Thesis report structure

EXPLORATION

3. E-government Infrastructure

Exploration is part of the *Problem Formulation* phase. It deals with understanding the concept of e-government infrastructures for businesses, the technology and services of Digipoort, and the actors involved in the working of e-government infrastructure for businesses. In Chapter 3 and Chapter 4 we answer the first sub-question,

SQ 1: *What are e-government infrastructures for businesses?*

In Chapter 3 we discuss e-government in general and in Chapter 4 we discuss Digipoort, an e-government infrastructure for businesses provided by the Dutch government. In this chapter, Section 3.1 explains the concept of e-government, Section 3.2 describes the categories of e-government, Section 3.3 describes the general architecture of e-government, Section 3.4 describes the rising complexity of e-government implementations and the need to focus on their security and Section 3.5 presents a summary of this chapter.

3.1. E-government

E-government or electronic government is defined as the use of information and communication technologies to enable the daily administration activities of governments. It is an internet driven activity which improves access to government information, services and expertise for citizens, employees, businesses, and agencies (Carter & Bélanger, 2005). IT used in many ways to simplify and improve transactions between governments and other actors, such as people, businesses, and other governmental agencies is e-government (Moon, 2002). Many technologies like electronic data exchange, interactive voice response, voice mail, email, web service delivery, and public key infrastructure form a part of e-government (Moon, 2002). According to The Economist (2000), E-government includes four major aspects:

1) The establishment of secure intranet and central database for more efficient and cooperative interaction among governmental agencies.
2) Web based service deliveries that are accessible via the web in a convenient and secure form.
3) e-commerce application for more efficient government transactions.
4) Digital democracy for more transparent accountability of the government.

Governments provide e-government services to different types of users, namely citizens, businesses, employees of governments, and other government agencies (Carter & Bélanger, 2005). This leads to different categories of e-governments. The following section describes the various categories of e-government.

3.2. Categories of E-government

There are many categorizations in literature for e-government. One of the broader and more common classifications of e-governments is based on the difference in delivery models. The US General Accounting Office categorizes e-government as Government to Citizen (G2C), Government to Business (G2B), Government to Employees (G2E), and Government to Government (G2G) (Carter & Bélanger,

2005). Belanger & Hiller (2006) takes into account the complexities of government relationships and categorizes e-government into six categories namely Government with individuals – delivering services (GwIS), Government with individuals – political process (GwIP), Government with business as a citizen (GwBC), Government with businesses in the marketplace (GwBMKT), Government with Employees (GwE), and Government with Government (GwG). We refer to this categorization of e-government further in this report. In Section 2.1 we mentioned the two-way interaction between governments and businesses. Some literatures differentiate this interaction as Government to Business (G2B) and Business to Government (B2G) (Fang, 2002; Palvia & Sharma, 2007). E-government infrastructure for businesses can therefore fall into two categories, GwBC and GwBMKT which indicate G2B and B2G interactions respectively. Table 2 shows the categorization of e-government according to Belanger & Hiller (2006), and how it fits in the broader categorization we mentioned earlier.

Table 2: Categorization of e-government, adapted from (Belanger & Hiller, 2006)

Category	Function	Type of Delivery
Government with individuals – delivering services (GwIS)	The government establishes a direct relationship with citizens to deliver a service or benefit, which can lead to two-way communications as individuals need information about benefits, and government may need information to process the benefits.	Government to Citizen (G2C)
Government with individuals – political process (GwIP)	The relationship between government and citizens as part of a democratic process, which might include voting online, participation in regulatory processes etc.	Government to Citizen (G2C)
Government with business as a citizen (GwBC)	The relationship shows the capacity for businesses to behave like citizens. Paying customs, taxes online could be examples of this type of relationship.	Government to Business (G2B)
Government with businesses in the marketplace (GwBMKT)	A major portion of the online transactions between governments and businesses involve procurement, contracting, and acquisition of goods and services by the government. E-procurement is an example of this type of relationship.	Business to Government (B2G)
Government with Employees (GwE)	The relationship between the government agencies and their employees are analogous to what the businesses have with their employees. The intranet used to provide information to the employees, and perform transactions with the employees is an example of this type of relationship.	Government to Employees (G2E)
Government with Government (GwG)	This relationship shows the collaboration between the different government agencies to provide services to one another.	Government to Government (G2G)

3.3. General Architecture

In this section we discuss the general architecture of e-governments. Riad, El-Bakry, & El-Adl (2011) conducted a survey on the various e-government architecture frameworks and found that countries develop their e-government plan depending on their strategy and user satisfaction parameters. However, there are intersections between the frameworks in terms of the layers in the architectures. Ebrahim & Irani (2005) developed an integrated framework for e-government that represents the

alignment of IT infrastructure with business process management in public sector organizations. They divided the architecture framework into four layers, access layer, e-government layer, e-business layer, and infrastructure layer as shown in Figure 3. The four layers are hierarchically implemented and are logically connected to allow two way transmissions of data and services. The four layers of the general architecture framework of e-government developed by Ebrahim & Irani (2005) are discussed below:

- *Access layer*
  Access layer consists of the various channels that the users use to access the government services. Users can include citizens, businesses, government departments, employees, and other community members. Some of the common channels that are used by the users include mobile phones, digital TV, call centres, kiosks, PCs, tele conferencing, and the web.

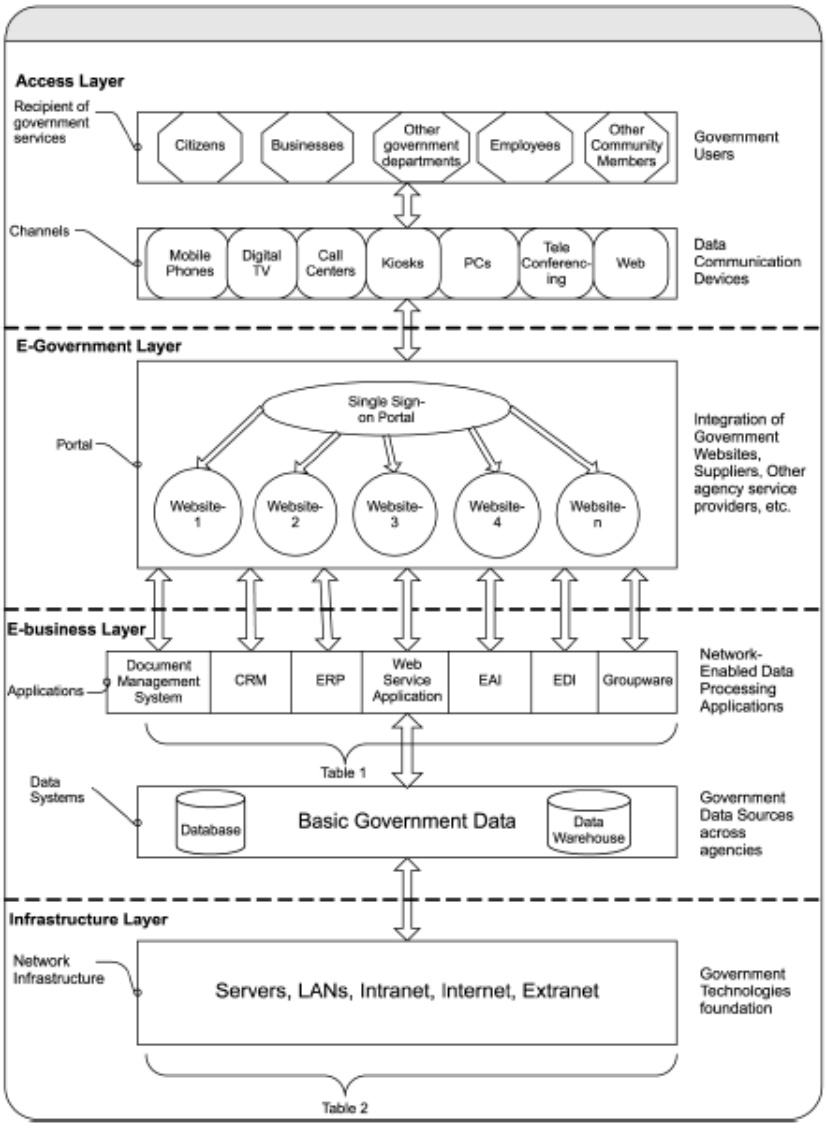

Figure 3: Framework of e-government architecture, adopted from (Ebrahim & Irani, 2005)

- *e-government layer*
  In many cases, e-governments use an integrated portal to provide a one stop shop for the users to the various services provided by governments. The use of an integrated portal will reduce the effort that users need to access different services. It reduces overhead and improves information flow. Though there are many advantages to having an integrated e-government layer, Ebrahim & Irani (2005) mentions that due to the organizational, functional and technical complexities associated with creating a single government portal, this layer is still in the infancy stage in many cases.

- *e-business layer*
  This layer consists of the ICT applications and tools such as existing databases and data warehouses that integrate front-end e-government layer applications with back end activities. The traditional standalone applications and databases of government departments that are not connected to other government departments create barriers between organization systems and processes. This layer implies the connectedness and communication between the computer systems and applications of different government departments in the e-government.

- *Infrastructure layer*
  The infrastructure layer consists of the technology infrastructure that reaches out to the different parts of the public sector organization and supports the three aforementioned layers. This layer focuses on the technologies that need to be implemented to provide safe and reliable e-government services to the customers. Technologies like LAN, servers, internet, intranet, and extranet are part of the infrastructure layer.

3.4. Increasing Complexity of E-Governments

We discussed a general architecture for e-governments above. However, it cannot be considered as a common blue print for all the e-government implementations across different countries in the world. E-government evolves along with a country's needs and implementation capabilities (Hanna & Qiang, 2009). The implementation of e-governments can differ from one country to another, depending on the differences in working cultures, skill sets, access to technology, and relevant infrastructure (Danish, 2006). Contemporarily, differing economic situations lead to political pressure on government agencies to do 'more with less'. Citizens and businesses expect higher service levels in their interaction with the government (Bharosa et al., 2015). Governments are focusing on using ICT as a tool to enable public agencies to change from routine-based, command-and-control organizations to knowledge-based, networked organizations that are externally focused on service. Government agencies often lack the in-house expertise to simultaneously define a country's ICT requirements, cost effectively implement the hardware and software, and maintain service levels. Given this scarcity of skills, e-government development, facilitation, and technical support functions are often shared across agencies or provided by the private sector. This leads to the development of government wide information infrastructure, shared networks, data centers, common business processes, and one stop service delivery centers (Hanna & Qiang, 2009). This is in line with the OECD vision for e-governments of the future (OECD, 2008). Governments often create an ICT agency outside the ministerial structure to overcome sectoral

silos and civil service constraints, to enable this complex implementation and engage various stakeholders and agencies involved (Hanna & Qiang, 2009). For instance Logius is such an ICT agency which takes on the role of managing the ICT services of the Dutch government. In the case of Digipoort, Logius performs the role of a Shared Service Center (SSC) which operates the multi-sided platform and provides operational and chain coordination services. Logius manages the chain of information flow from the businesses to the governments, while also ensuring that the service level agreements (SLAs) with the vendors (external and internal) providing the hardware and software services are met (Bharosa et al., 2015). The Digipoort case is discussed in detail in the next chapter.

Our analysis above reiterates the difficulty in representing e-government implementations through a generic architecture framework like the one suggested by Ebrahim & Irani (2005). E-government implementations are rising in complexity and functionality. Governments are moving towards a more open model of design, production and delivery of online services, taking advantage of the possibility offered by collaboration between citizens, entrepreneurs and civil society (European Commission, 2010). With governments moving from a traditional silo thinking to modular implementation, and striving to provide ICT enabled public services to citizens and businesses, the need to enhance security, privacy and trust in e-government services is well recognized (Jacobi et al., 2013). We therefore restate the need for government organizations to keep up to date the threat landscape of their e-government infrastructures.

3.5. Summary

In this chapter we described e-government, its categorization, and the general architecture of e-governments. E-governments use information and communication technologies to enable the daily administration activities of governments. E-governments are categorized according to the relationship of governments with different consumers into six categories as shown in Table 2. E-government infrastructure for businesses can fall into two categories, Government with business as a citizen (GwBC) and Government with businesses in the marketplace (GwBMKT) depending on the type of services used by businesses. We also discussed the general architecture of e-governments according to Ebrahim & Irani (2005). The implementation of e-governments however differs among countries due to the differences in cultures, skill sets, and access to technology, and relevant infrastructures. There is a need for enhanced security of e-government infrastructures as the complexity of e-government implementations rise. This reiterates the need for understanding the threat landscape of e-government infrastructures. In the following chapter we look at the case of Digipoort as an exemplar of e-government infrastructure for businesses.

4. Case Description – Digipoort

Chapter 3 described the characteristics of e-government in general. In this chapter we discuss the case of Digipoort – an e-government infrastructure for business enterprises provided by the Dutch government and managed by Logius. Digipoort is the focus of our research and is referred to in abundance in the Design and Application chapters of this report.

Digipoort is an ICT infrastructure of the Dutch government which handles the message traffic to and fro government agencies. It helps businesses in automating the process of sending large numbers of reports, returns, and other information to the various government agencies. Around 71.5 million messages were sent through Digipoort in 2012 (Logius, 2015f). It provides a common infrastructure for information interchange between businesses on the one hand and government agencies on the other. Much of the information that is sent through Digipoort is related to customs information for the *Douane* (Dutch customs office), and tax information for the *Belastingdienst* (Dutch tax office). Digipoort is also used for sending financial reports to the tax authorities (Belastingdienst), sickness and recovery reports to the Uitvoeringsorgaan Werknemers Verzekeringen (UWV), exchanging e-invoicing (e-Factureren) details, and automated purchasing & invoicing details through DigiInkoop etc (Logius, 2015i). Digipoort therefore can be classified under the 'GwBC' and 'GwBMKT' category of e-governments due to the fact that businesses use Digipoort both for supplying information mandated by law and also for online market transactions. We already discussed the different categories of e-governments in Section 3.2.

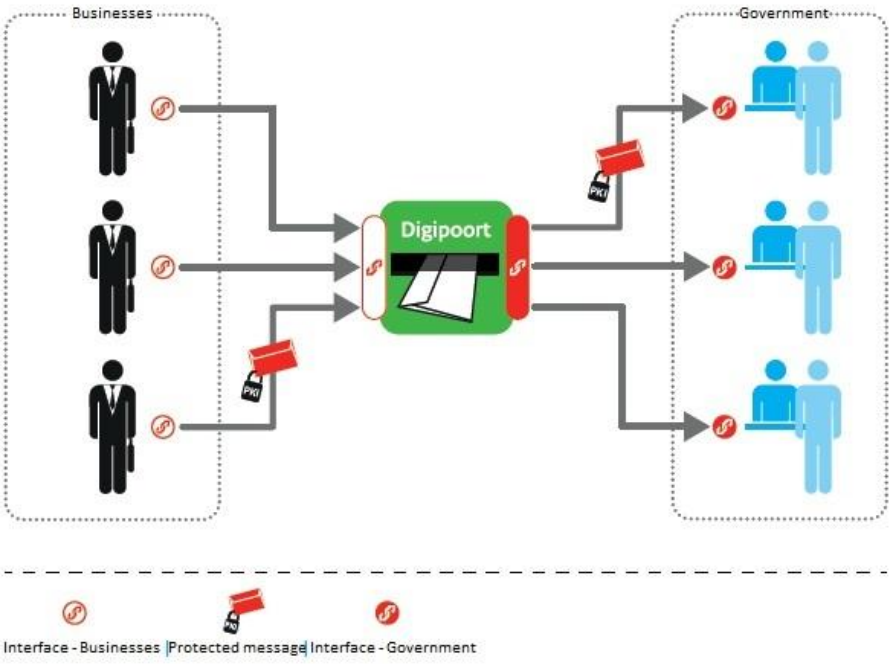

Figure 4: Digipoort as a link between businesses and government

Digipoort makes exchanging data simpler, because companies have one electronic interface to provide their data for various government agencies. Digipoort ensures that it is delivered to multiple

government parties. The result is a reduction in administrative burdens for businesses. A large number of steps involved in the processing of high volumes of messages to the government agencies are redundant. Automating those processes help save valuable time, costs, manual processing work, and also improves accuracy and safety (Logius, 2015p). Figure 4 shows how Digipoort acts as a link between businesses and government agencies. All these advantages make Digipoort an important e-government service of Logius and the Dutch government.

Types of Digipoort

Digipoort is an umbrella term used to identify the two different messaging systems maintained by Logius. One is Digipoort OTP (Overheidstransactiepoort or Government Transaction Gateway), and the other is Digipoort PI (Process Infrastructure). Although there are several similarities between them in terms of set up and the overall functionality they are two technically separate process infrastructures. The two infrastructures offer completely different interfaces for connecting with the Digipoort platform. An interface is defined as a system-to-system connection between information systems that facilitates the exchange of information (Bharosa et al., 2015). Digipoort OTP lets its users connect to the platform using X.400, SMTP, FTP and POP3 interfaces, while Digipoort PI offers interfaces such as SOAP, WUS and EbMS. Both the infrastructures perform the task of transferring information between businesses and the government.

In Section 4.1 we discuss in detail about Digipoort OTP and its various services. We also analyze the use cases of Digipoort OTP to understand the user-system interactions in Digipoort. In Section 4.2 we discuss Digipoort PI in detail and explain the infrastructure and services of Digipoort PI. Furthermore in Section 4.3 we discuss an important enabling technology for the security of e-governments – the Public Key Infrastructure (PKI). Subsequently we also present of a summary of this chapter and a reflection on the sub-question 2 in Section 4.4.

4.1. Digipoort OTP

The Digipoort (Overheidstransactiepoort or OTP) is an electronic post office for businesses, from the government. It provides a common platform for information interchange between the businesses on the one hand and the governments on the other. When a company sends an envelope with address (electronic message), Digipoort looks into the header of the message and identifies the government agency for which the report is intended to. Then Digipoort delivers the message with the correct files to the correct recipient(s). For each transmitted envelope, it is checked whether the sender is known and is authorized to send data to the receiver(s). Digipoort OTP provides a number of interfaces on either side of the platform that helps the users on both sides to connect to the platform. The current Digipoort OTP has possibilities for connecting through the following interfaces:

- *SMTP - MTA (for businesses and governments)*
  SMTP - MTA (Mail Transfer Agent) requires the delivering party to have access to a fully functioning SMTP server, an SMTP server that can send and receive SMTP messages. Return messages are delivered directly to the SMTP server from the delivering party via a secure

session. A leased line or VPN connection is used to securely connect to Digipoort using this interface.

- *SMTP - MSA and POP3 (for businesses)*
  Not all the companies who want to exchange messages with governments through Digipoort have access to a continuously available server. To make it easier for businesses that want to use Digipoort for sending messages over the Internet, the SMTP protocol is made use of, in combination with POP3. The company can send messages via SMTP MSA (Mail Submission Agent) server and receive via the POP3 protocol. The security of the two message flows takes place over an encrypted connection, based on TLS / SSL. Authentication of the companies is done through a user ID and password. The authentication to the server side (SMTP and POP3-MSA) is performed by means of a server certificate.

- *X.400 P1 (for governments)*
  The X.400 P1 interface on Digipoort is another messaging protocol that was being used by Digipoort. On the business side, the X.400 P1 is being phased out and will no longer be available as an interface in Digipoort OTP. Presently, only the Customs (*Douane*) uses X.400 P1 as an interface for the government side systems.

- *FTP (s) (for businesses and governments)*
  The FTP (s) or *File Transfer Protocol* interface is designed to exchange large files between business and government and is accessible via the Internet. The FTP (s) interface plays the role of FTP (s) server. Both businesses and governments can upload files to the server and retrieve it. Each FTP (s) user (business or government) hereby has access to its own private environment. The routing of the files from the sender to the receiver is done by the FTP (s) server on the basis of information supplied by the sender metafile. The metafile contains, among other information, the recipient's name and the original filename. Authentication of an FTP (s) user takes place on the basis of a client certificate in conjunction with a user ID and password. Authentication of the FTP (s) server occurs by means of an FTP (s) server certificate.

Figure 5 shows a schematic representation of the interfaces available to businesses and governments (Overheid) in Digipoort OTP. Appendix I provide more details on the different types of email protocols.

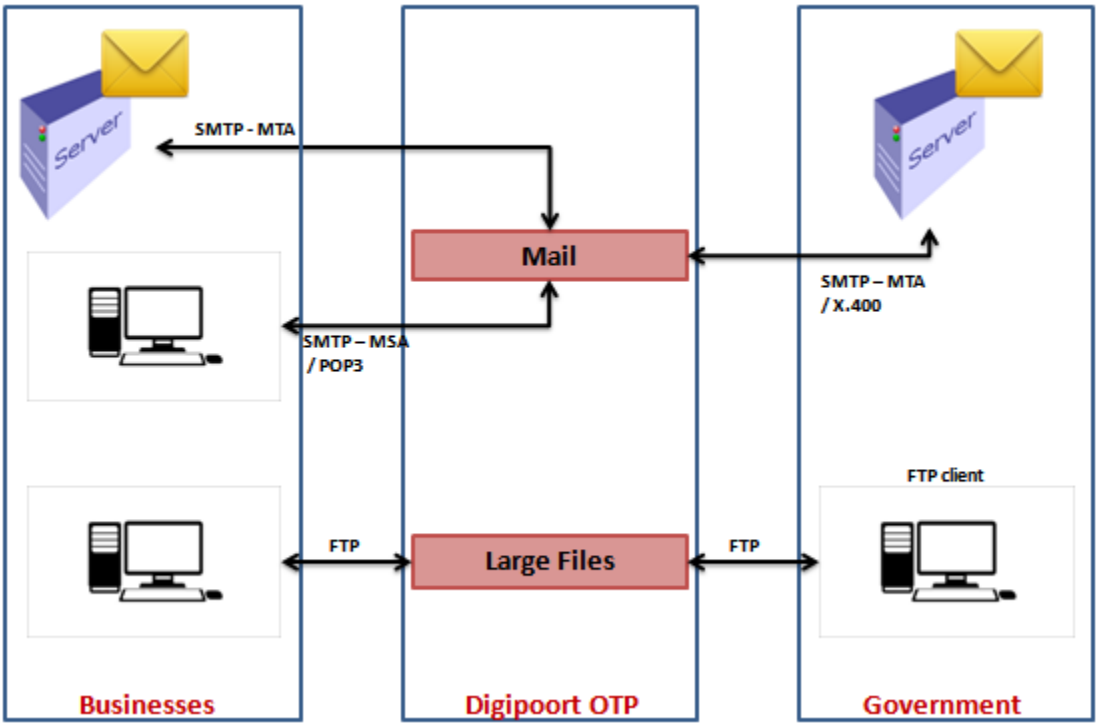

Figure 5: Digipoort OTP interfaces

4.1.1. Digipoort OTP - Services

Digipoort OTP provides its services to different users (businesses) and government agencies. The most important message service streams through Digipoort OTP are discussed below. Of these, the OTP service to the Douane (Customs) is the biggest and the most important one. The following services are offered by Logius through Digipoort OTP:

Sending information to Douane (Customs)

Table 3 shows the various data exchange details about Douane. A major portion of the messages sent by businesses through Digipoort OTP is concerned with Douane. SMTP interface handles more than 95% of the communication, majority of which is for exchanging customs declarations with Douane. The businesses connect to Digipoort directly or through an intermediary (HUB). The interfaces used are SMTP – MTA or SMTP – MSA with POP3. The SMTP – MSA & POP3 are usually used by businesses that do not have the circumstances to house a dedicated SMTP server. The messages are sent over the internet using SMTP – MSA and messages are received using the POP3 interface. On the other side of Digipoort OTP, Douane connects using a comparatively older interface called X.400. Because of the difference in interfaces between the messages sent and received, the Digipoort OTP handles the translation of messages from one interface to another.

Table 3: Douane data exchange details, adopted from (Logius, 2015c)

Sender	Government Agency	Message Type	Interface	Connection
Companies	Customs	Declaration Statements	• SMTP–MTA • SMTP–MSA/ POP3	• Direct • Intermediate/ HUB

Sending information to Belastingdienst (Tax)

The Belastingdienst (Tax authority of Netherlands) uses Digipoort for data delivery from financial institutions (Table 4), and VAT refund submissions for entrepreneurs (Table 5). The interface used in this case is FTP.

Table 4: Data delivery of financial institutions to the tax department, adopted from (Logius, 2015e)

Sender	Government Agency	Message Type	Interface
Financial Institutions (banks & insurance)	Tax	• Banking and investment products • Insurance	FTP

Table 5: Data delivery of entrepreneurs to Tax, adopted from (Logius, 2015j)

Sender	Government Agency	Message Type	Interface
Entrepreneurs	Tax	Restitution Request EU – VAT	FTP

Sending information to NVWA

Table 6 shows details about the data exchange with NVWA. Digipoort OTP is used by fishing vessels to inform the Nederlandse Voedsel- en Warenautoriteit (NVWA) about the catch details. It is also used by businesses of food and consumer products to send import details to the NVWA. NVWA is the Netherlands Food and Consumer Product Safety Authority. The interfaces used include SMTP – MTA or SMTP – MSA & POP3.

Table 6: Data exchange of businesses to NVWA, adopted from (Logius, 2015g)

Sender	Government Agency	Message Type	Interface	Connection
Companies	NVWA	• E-logbook fishing vessels • Client import	• SMTP–MTA • SMTP–MSA/ POP3	• Direct • Intermediate/ HUB

Sending information to the De Nederlandsche bank (DNB)

Table 7 shows the details about the data exchange with DNB. The financial institutions like banks and insurance agencies use Digipoort OTP to send financial information to the DNB. The interface used is FTP.

Table 7: Data exchange of financial institutions to the DNB, adopted from (Logius, 2015d)

Sender	Government Agency	Message Type	Interface
Financial institutions: banks and insurers	De Nederlandsche Bank	Deposit Guarantee Scheme (DGS)	FTP

In the next section we study the use cases of Digipoort OTP with respect to the service it provides for Douane, in order to understand the interaction of Digipoort with its various stakeholders.

4.1.2. Digipoort OTP for Douane – Use Cases

Use cases allow us to describe a set of events that when taken together will lead to a system doing something useful. A use case model includes not only use cases but also actors. The use case model shows us how the actors interact with the system and how they collaborate in a sequence of actions (Bittner & Spence, 2002). We developed several use cases of Digipoort OTP being used by businesses to communicate with the Douane. 95% of the messages sent through Digipoort OTP are related to the Douane. The other message streams are similar to Douane, only sometimes differing in the type of interface used. This is the reason why Douane is considered as a representative of the Digipoort OTP service and used to build use cases here. The use case models will be used for understanding the ways in which Digipoort is used and the interaction of various actors with the Digipoort system.

Reporting Party Sends Message to Douane using SMTP – MTA

Figure 6 shows how the reporting party connects to Digipoort using SMTP – MTA interface and uses it to send a message to Douane. The reporting party can be a business customer or an intermediary who wants to send information to Douane. Intermediaries or HUBs help businesses (usually smaller ones or small fishing boats) in sending messages to Digipoort. For e.g. Portbase is an intermediary for Digipoort OTP. The reporting party is authorized using the authorization database which contains the details of white-listed customers who can send messages through Digipoort OTP. This database is maintained by the vendor through a process called Provisioning. The message sent is handled by the Digipoort OTP core. The OTP core is a black box with several functionalities to handle the message, including receiving, translating, storing, and sending messages. The Douane uses the X.400 interface for messages, and therefore the OTP core translates the message from SMTP to X.400. Log files are created for each step and are stored in the logging database (Logging DB).

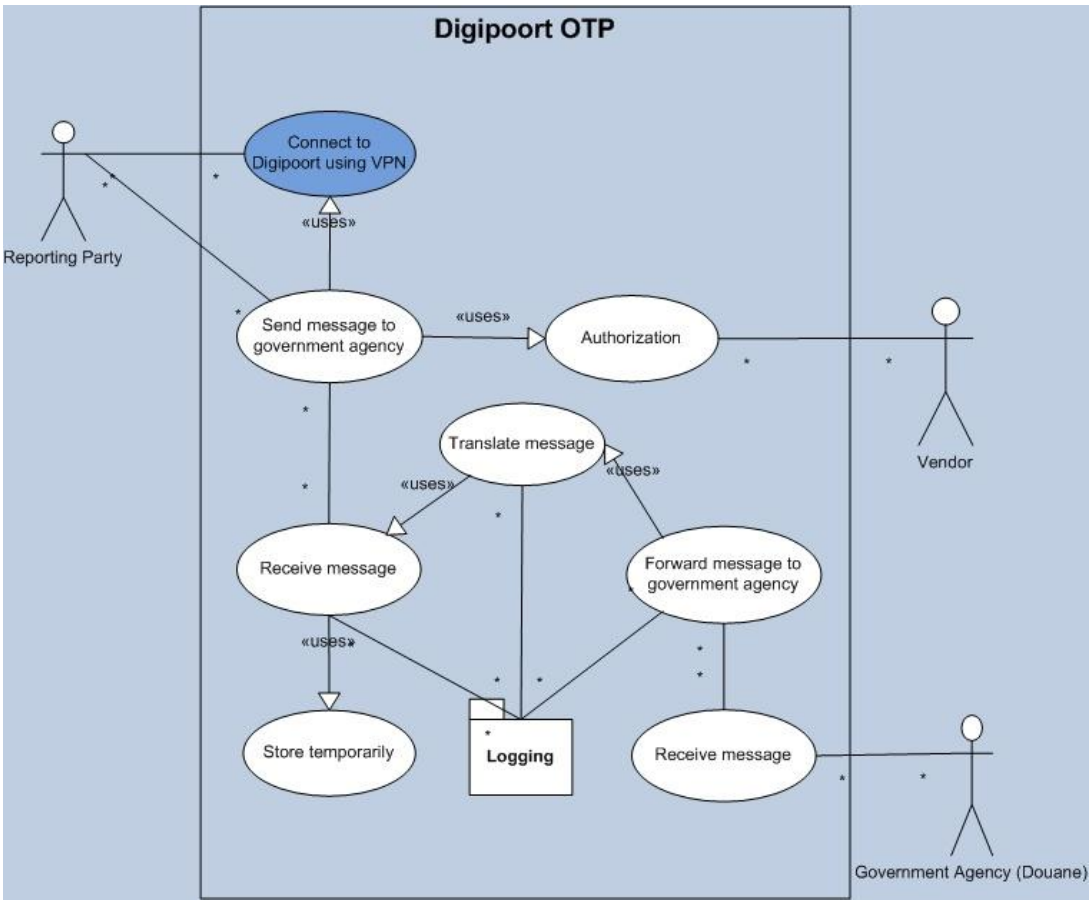

Figure 6: Use case diagram – Reporting Party sends message to Douane using SMTP - MTA

Douane Sends Message to Reporting Party using SMTP – MTA

Figure 7 shows the interaction between Douane, the reporting party and the Digipoort system. The Douane sends status information of the messages received, back to the reporting parties. The government agencies can connect to Digipoort using the intranet of the Dutch government known as the Diginetwerk. The Douane uses X.400 interface and therefore the messages need to be translated to SMTP – MTA interface for the reporting party.

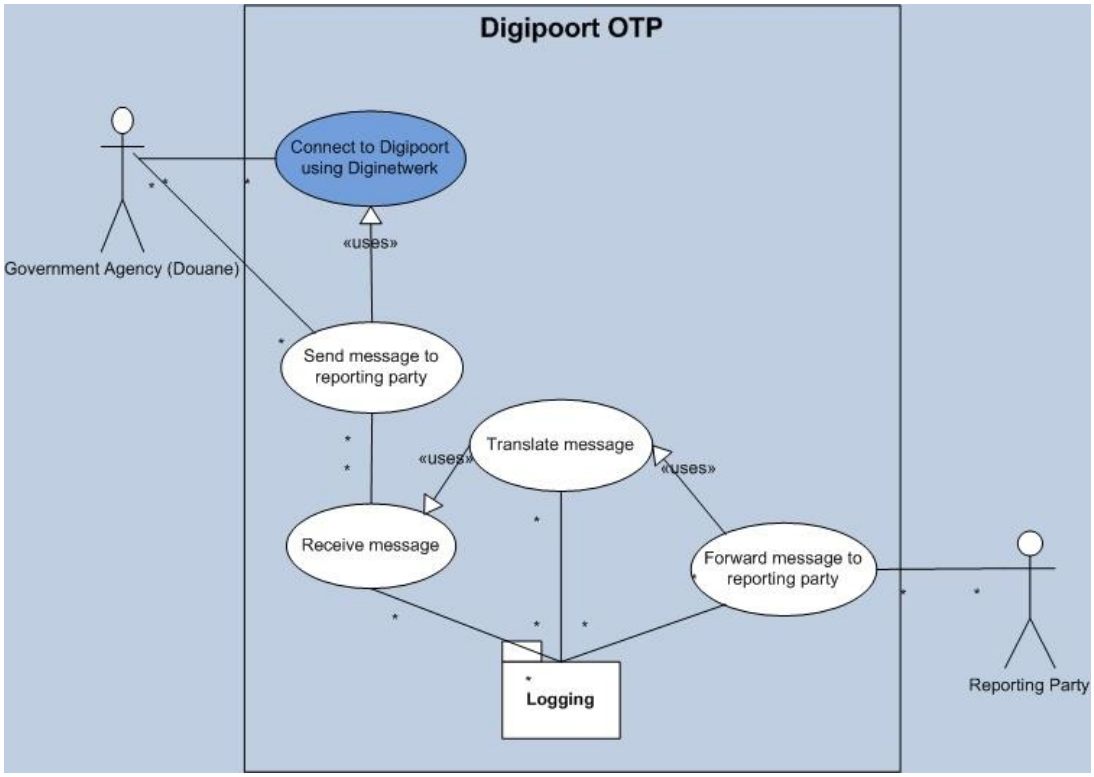

Figure 7: Use case diagram - Douane sends message to reporting party using SMTP - MTA

Reporting Party Sends Message to Douane using SMTP – MSA

Figure 8 shows how the SMTP – MSA interface is used by businesses over a TLS connection to send messages to the Douane. A Trusted Third Party (TTP) is involved in this case. Trusted Third Parties or Certification Service Providers (CSP) are external agencies which issue PKI certificates to send information securely over the internet. We discuss PKI and digital certificates later in this chapter. Using PKI certificates, the information sent over the internet is protected with a high level of reliability. The PKIOverheid (Public Key Infrastructure service by Logius) ensures reliable electronic communication within and with the Dutch government, by acting as the root Certification Authority (Logius, 2015l). The customers are expected to obtain the certificates from the CSP's before they can connect to the Digipoort. Authorization is performed using an authorization database which is maintained by the vendor. This is part of the Provisioning process, which is an important function of the vendor and is also discussed in the use cases of the vendor. The other use cases included in this use case model mainly concerns with translating, temporarily storing, logging, and sending or receiving the messages. These activities are performed by the Digipoort OTP core. The working of the OTP core is however out of the scope of this report.

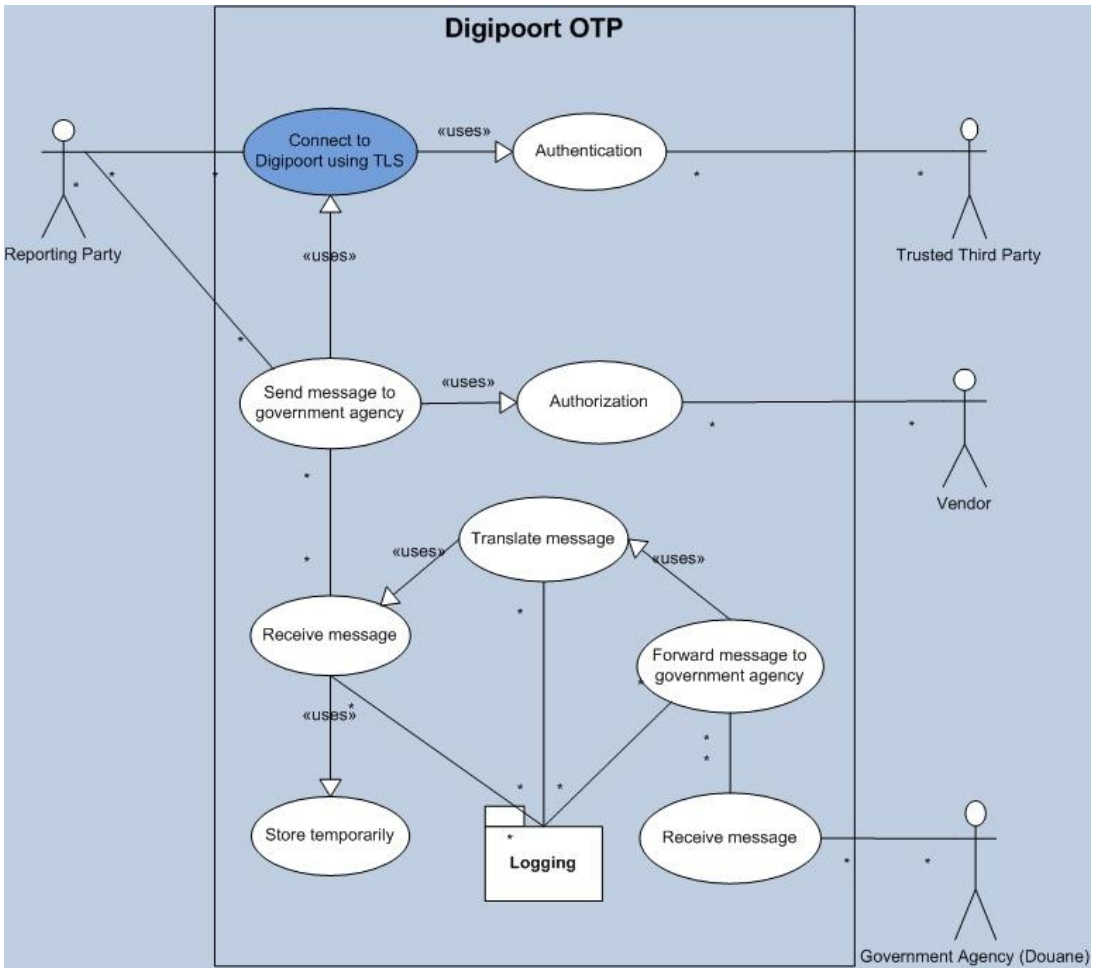

Figure 8: Use case diagram – Reporting Party sends message to Douane using SMTP - MSA

Reporting Party Accesses Message Sent by Douane using POP3

Figure 9 shows how the POP3 interface is used by the reporting parties (business & intermediaries) to access the status messages sent by the Douane. The reporting party connects using a TLS connection to the POP3 message store to get the messages. The other actors involved in this use case model include the TTPs for maintaining the digital certificates, and Vendor for provisioning of the Authorization DB.

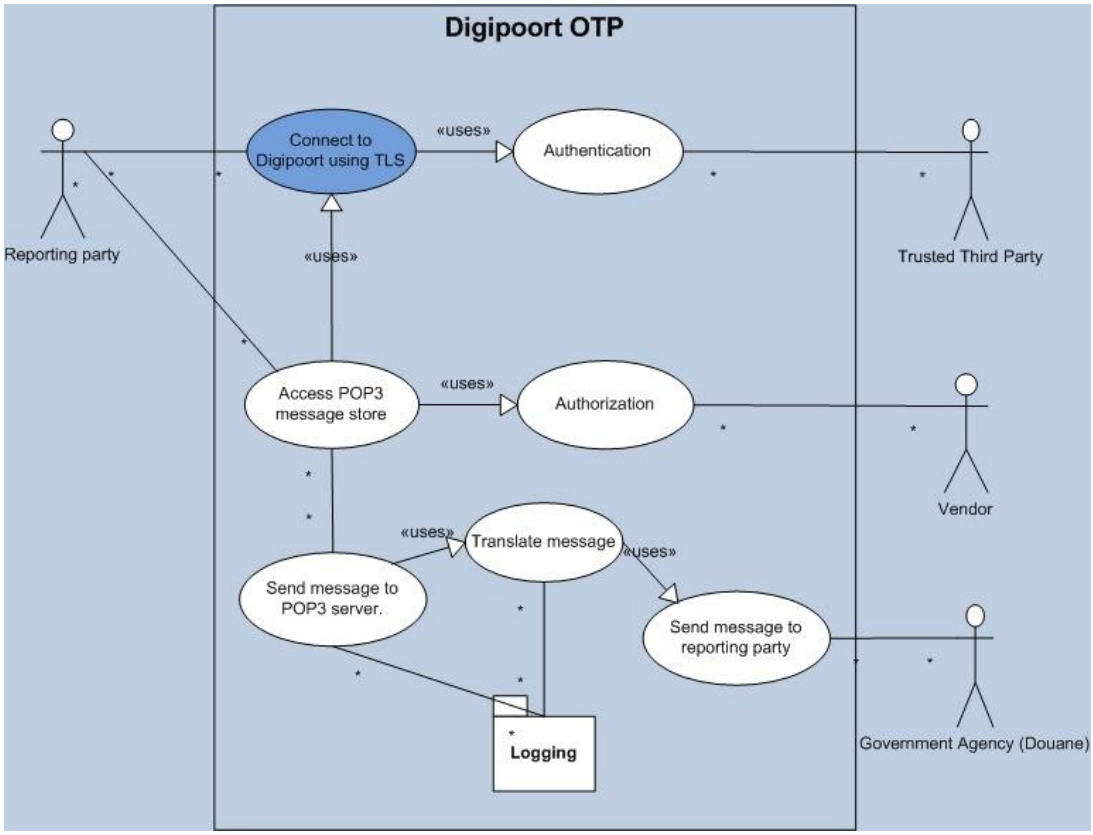

Figure 9: Use case diagram - Reporting party accesses message sent by Douane using POP3

Vendor Functions - Re-Inject Message

Figure 10 shows the various use cases of a vendor. The vendor performs several functions on Digipoort. One of the main functions of the vendor is *Provisioning*. It involves maintaining all the authentication and authorization databases of Digipoort OTP. Servicing, monitoring, managing the archiving and logging is also performed by the vendor. The vendor generates reports on system performance, which are sent to the service managers at Logius, according to the Service Level Agreement (SLA).

Another important function performed by the vendor is the re-injection of messages. In some cases, the Douane will request the *Ketenbeheerder* (Chain manager) at Logius to re-inject a previously sent message, from the temporary storage. The chain manager raises a request with the vendor to re-inject the message in question. The request is then executed by the vendor. The messages are usually stored in the temporary storage for 72 hrs. Because of the variety of their functions, and their direct interaction with the Digipoort system, the vendor is one of the most important actors with respect to Digipoort.

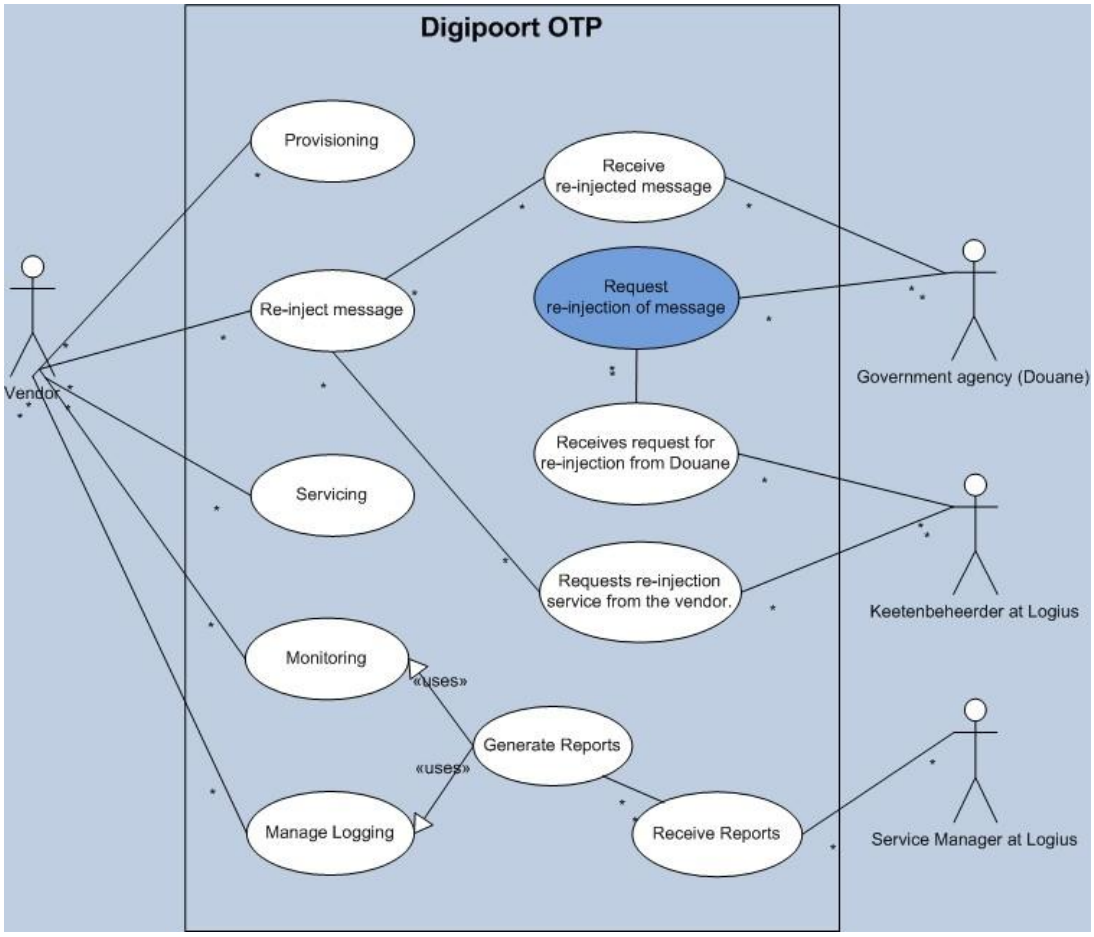

Figure 10: Use case diagram - Vendor functions and re-inject message

In the use case models of Digipoort OTP discussed above, we demonstrated how the businesses and intermediaries send and receive messages from the government agencies. We also showed the interaction of actors like Trusted Third Parties and Vendors with the Digipoort OTP system. Similar use case models can also be developed for other services of Digipoort OTP. The use cases and the interaction of actors with the Digipoort system will remain more or less the same for them too. Moreover, a major share of messages sent through Digipoort OTP by reporting parties are directed at Douane. We therefore consider the use case models of Douane as a fitting representation of the Digipoort OTP system.

In this section we described the first type of Digipoort - Digipoort OTP, its services and the use cases of the Digipoort OTP service for Douane. In the next section we discuss the second type of Digipoort - Digipoort PI, its technology and services.

4.2. Digipoort PI

Digipoort PI is an important generic infrastructure that Logius provides for standard data transfer processes between the government agencies and the businesses. It is mainly used for providing services related to Standard Business Reporting (SBR), eFactureren (e-invoicing) and DigiInkoop (Purchasing). The

SBR service is mainly used by businesses to send information to government agencies like Belastingdienst (Tax), CBS (Statistics Netherlands), and KvK (Chamber of Commerce Netherlands). The main difference between the SBR and eFactureren or DigiInkoop is the messaging standard used. SBR uses the XBRL (eXtensible Business Reporting Language) messaging standard, while eFactureren and DigiInkoop use UBL OHNL and SETU (HR-XML) OHNL messaging standards. XBRL is an internationally accepted standard for the structure and use of taxonomies for reporting (Bharosa et al., 2015). The UBL OHNL standard is a specification of the international UBL (2.0) standard. The standard describes the messages sent by businesses regarding the purchasing of all products and services with the exception of staff hiring (Logius, 2015s). SETU (HR-XML) OHNL is a standard that describes the messages Logius use in the context of data interchange for hiring temporary staff (Logius, 2015q). These variants are designed to deliver electronic invoices to the government. Both UBL OHNL and SETU (HR-XML) OHNL are maintained by Logius.

Digipoort PI is managed by Logius employing the services of internal and external vendors. Internal vendors are the departments of Logius who are involved in the functioning of Digipoort PI. Infrastructure & Services (I&S) Managed Services (MS), a vendor responsible for the process management and Infrastructure & Services (I&S) Center for Standards (CvS) responsible for managing the data classification dictionary of Digipoort PI are the two main internal vendors. External vendors are mainly involved in providing and maintaining the software and hardware assets of Digipoort PI. VENDOR1[1] develops and manages the software and the Digipoort PI platform, while VENDOR2[2] manages the infrastructure (servers, datacenters etc) of Digipoort PI. The management of the vendors and the whole information chain from businesses to the government agencies of Digipoort PI is performed by the *Keteninformatiediensten* (Chain Information Services) department of Logius. The *Keteninformatiediensten* (KD) is also responsible for ensuring sufficient reliability and confidentiality of the electronic message transfer between the chain partners (Bharosa et al., 2015).

The working of Digipoort PI involves several enabling technologies like Web Services, Interface Standards, and the PKI (discussed in Section 4.3). In the following section we give a general description about the Web Service technology and in Section 4.2.2 we will explain the Web Services and Interfaces used by Digipoort PI.

4.2.1. Web Service

Digipoort PI offers different services to companies and governments in the form of web services. Web service refers to a specific functionality for the transformation of input information to output information, which can be invoked by using certain standards. According to the World Wide Web Consortium (W3C), web service is defined as:

"*A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages,*

[1] The name of the software vendor is not revealed to protect confidentiality.
[2] The name of the infrastructure vendor is not revealed to protect confidentiality.

typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards." (W3C, 2004)

Using standards like SOAP (Simple Object Access Protocol), HTTP and XML, a web service is used for information exchange between different systems. It can also activate an application and receive its result as a return message. A Web Services Protocol Stack consists of layers of internet protocols or standards used to design, discover and implement web services. The major components of a Web Service Protocol Stack as shown in Figure 11 are:

- *Transport Layer*

  The transport layer transfers messages between applications. HTTP is used for addressing and communication between a web client and a web server.

- *XML Messaging Layer*

  This layer encodes the messages with the XML standard and writes the message using SOAP standard.

- *WSDL Layer*

  The WSDL (Web Service Description Language) standard is used for defining service interfaces.

- *UDDI Layer*

  The UDDI (Universal Description, Discovery and Integration) is used as a library for finding services.

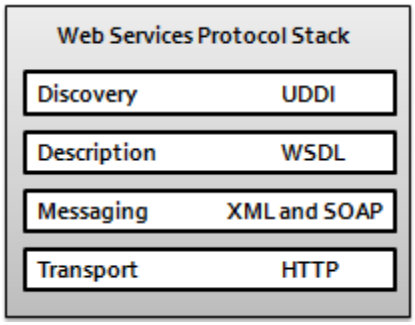

Figure 11: Web Services Protocol Stack, adapted from (W3C, 2004)

We gave a general description of Web Service technology in this section. In the following section we describe the infrastructure and services of Digipoort PI. We will also look at the various Web Services used by Digipoort PI.

4.2.2. Digipoort PI - Infrastructure and Services

Digipoort PI offers various services targeted at the companies and the government. They are not only services that help in the transfer of information but also in the authorization and validation of the businesses who send the information. Figure 12 shows the four main parts of Digipoort PI – Interfaces, Web Services, Process Functionality, and Internal Services. All these parts together are known as the Process Infrastructure or the Generic Infrastructure.

Interfaces

The interfaces that Digipoort PI supports are shown in Figure 12. An interface is defined as a system-to-system connection between information systems that facilitate the exchange of information (Bharosa et al., 2015). Digipoort PI provides two interfaces for communication, namely WUS and ebMS. WUS is an acronym for WSDL, UDDI, and SOAP. It is an open standard used by Digipoort PI for making the sending of messages between businesses and Digipoort possible (Logius, 2015k). Digipoort uses the interface Digikoppelling WUS 2.0 standard for queries from government organizations to Digipoort (Logius, 2015k). Digikoppelling is a service of Logius which includes a set of interface standards that can enable a government agency to exchange messages with all the other government agencies and connect virtually to every e-government component (Logius, 2015h). Similarly Digipoort also uses the interface standard Digikoppelling ebMS for asynchronous messaging between government organizations and Digipoort. Asynchronous traffic includes messages for which an immediate response cannot be given. This interface is also part of Digikoppelling service provided by Logius (Logius, 2015h).

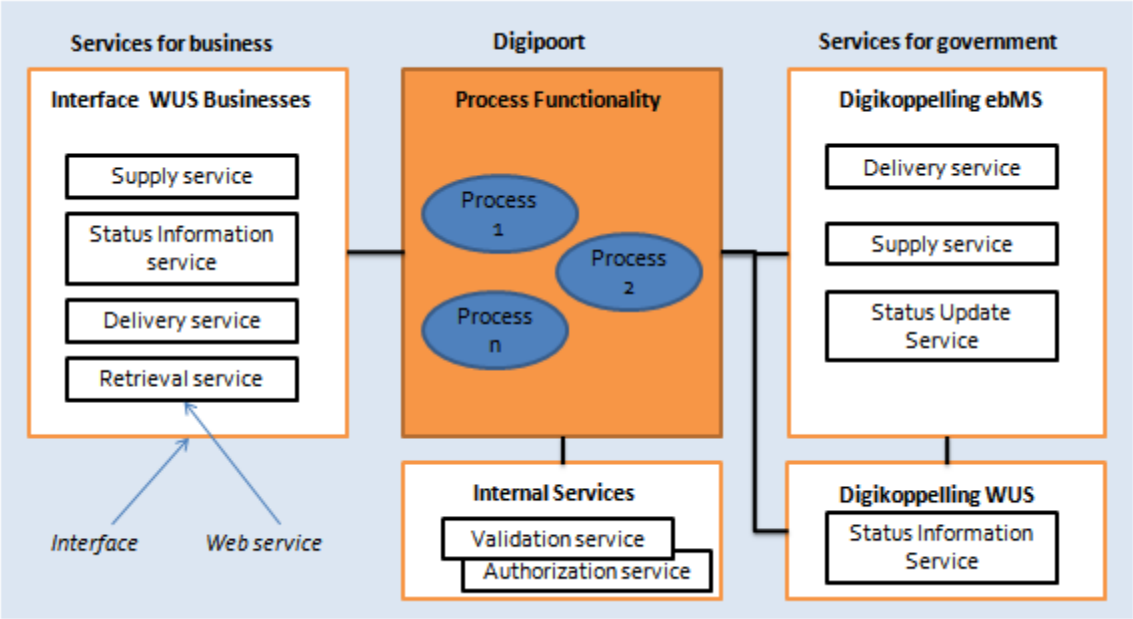

Figure 12: Services provided by Digipoort PI

Web Services

The Digipoort PI uses several web services for transferring information between the businesses and governments. These include:

- *Supply Service*

  The Supply Service, also called the Aanleverservice is a web service provided by Digipoort PI to the companies to send messages to the government organization who is the recipient. The Supply Service validates the Supply Request according to the WUS open standard, accepts the validated Supply Request, determines which process functionality is to be performed on the message, places the Supply Request, and sends the Supply Response when the stipulated requirements are fulfilled.

- *Delivery Service*

The Delivery Service is used by Digipoort to deliver messages supplied by a government party to a business. The Delivery Service, unlike the other web services is set up by the businesses. The Delivery Service validates the Delivery Request, processes the Delivery Request and sends the Delivery Response. Digipoort sends the Delivery Request using a pre-defined structure that is specified in an XML diagram (XSD) incorporated in the WSDL that formally describes the Delivery Service.

- *Status Information Service*

This service is used to request status information from Digipoort. Status information is the information about the progress in handling of a specific message. At each step of the process, Digipoort records a status. The businesses can request this information using the Status Information Service.

- *Retrieval Service*

The Retrieval Service is used by the businesses to request messages from the Digipoort. Government organizations supply messages related to the data that was sent in the past by businesses, to Digipoort. For instance, this could be a response to the assessment submitted by the company to a government agency. The business can submit a retrieve request and retrieve the messages related to them.

Process Functionality

The process engine allows for a message based execution of the various processes that are to be performed on the messages before it reaches the requesting party. This means that different business reports follow different process flows. For e.g. a VAT return is processed in a different way from a statistics report. This enables Digipoort PI to handle multiple types of messages, carry out various process configurations, and invoke different web services depending upon the type of the message. Different processes are related to handling of information for different government agencies. For e.g. Digipoort PI is used by the Belastingdienst for income reporting, DigiInkoop for getting information from suppliers, UWV for receiving sickness and recovery reports about employees from businesses, and E-factureren for receiving invoices from the businesses.

Internal Services - Authorization and Validation

Authorization and Validation are two of the auxiliary services provided by Digipoort PI. Authorization service is used to establish whether a reporting party is authorized to submit messages to the Digipoort. Digipoort consults a trusted approvals registry to check the authorization of users (Bharosa et al., 2015). The authenticity of companies is always established before the authorization. Authenticity is determined on the basis of PKIOverheid certificates which the reporting party requests from a CSP. The PKIOverheid client certificate that is located on the client system is used to open a connection with Digipoort PI in accordance with the TLS/SSL protocol. In addition to authentication, this protocol also offers encryption at the transport level. The Validation service validates the message sent by the companies. The message

is validated using a schema/model like XML schema definition (XSD), XBRL, or other standards like UBL OHNL.

In this section we discussed the Process Infrastructure of Digipoort PI. In the following section we give a short account of the structure of the SOAP message that is sent by businesses to the Digipoort PI.

4.2.2.1. Message Structure

The message flowing through Digipoort PI has a specific structure based on the interfaces used. The WUS 2.0 interface for companies uses the SOAP 1.1 standard for composing electronic messages. SOAP is a standard for electronic messaging based on services. A message that is sent to a service is called the ''SOAP Request'' and the response for the request is called the "SOAP Response". If errors are found upon receipt of or whilst processing the request message, a "SOAP fault" is returned.

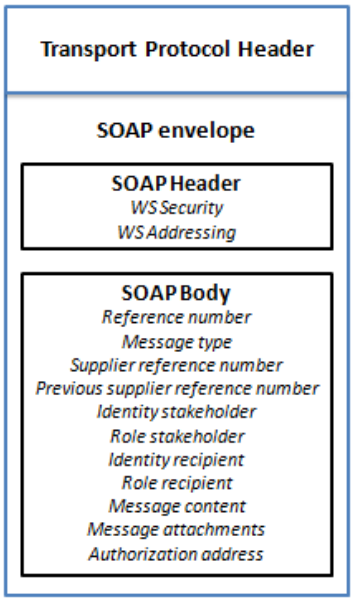

Figure 13: SOAP message structure, adopted from (Bharosa et al., 2015)

The structure of request and response messages depends on the service within which these messages are used. Figure 13 shows the structure of the SOAP request for the Supply Service we discussed earlier. A SOAP message consists of the following parts:

- *Transport protocol header*
  For transport of messages, SOAP generally uses HTTP and SMTP protocols.

- *SOAP envelope which contains SOAP Header and SOAP Body*.
  The SOAP Header consists of two elements WS Addressing and WS Security. WS Addressing is used for routing the messages and WS Security for digitally signing the messages. The sender has to digitally sign the body and header elements of a supply request. They have to be signed using an electronic signature, and using a PKIOverheid certificate issued by a CSP. The certificate, the signature and the algorithms that are used have to be included in the WS

Security elements in the header. WS Security helps in enforcing integrity and confidentiality of the messages independent of the transport protocol (Bharosa et al., 2015).

The SOAP Body contains the Supply Request. The functional data or the business document forms a part of this. The SOAP Body has several elements like the reference number, Message type, Supplier reference number, the Message content, the Message attachments etc. The content of the message can be in binary (such as a pdf document) or XML (such as XBRL or UBL) formats (Bharosa et al., 2015). The components of the SOAP Body might be different for different purposes. For instance, the SOAP Body of a SOAP Response has several different elements compared to the SOAP Body of the SOAP Request. Since we won't be discussing about the message type or content of the message in our threat assessment methodology, we will limit our discussion of the message structure here.

We mainly discussed Digipoort PI and its services in this section. We defined web services in general and discussed the type of web services handled by Digipoort PI. We also explained the other important parts of Digipoort PI like the Interfaces, Process Functionality and the Authorization and Validation services. The structure of a Supply Request message was also discussed above. We already mentioned the use of digital certificates and PKI in both Digipoort OTP and Digipoort PI. In the section below we give a short account on PKI and the security it provides to e-government infrastructures.

4.3. Cyber Security in e-Government

In this section we discuss the Public Key Infrastructure (PKI), a technology that plays an important role in providing security services including confidentiality, authentication, digital signatures, and integrity in e-government infrastructures. A PKI is a combination of hardware and software products, policies and procedures, used to provide the basic security required for secure communications so that users who do not know each other can communicate over a chain of trust (Hunt, 2001b). PKI is an enabler of Trust and provides cryptographic services, strong user identification, and non-repudiation among entities that interact with each other in the service (Kefallinos, Lambrou, & Sykas, 2006). A PKI system provides users of electronic communication services with digital key pairs, a private and a public key. The key pairs are associated with one or more certificates, corroborating to the identity or to the attributes of the certificate and the key holder (Logius, 2015m). The certificates or digital certificates are sometimes also referred to as X.509 certificates (Posey, 2005).

To enable trust, a PKI incorporates a collection of one or more Certificate Authorities (CAs) usually arranged in a hierarchy acting as the Trusted Third Parties (TTPs). The trust here is based on the certificate hierarchy as shown in Figure 14. The root certificate, the first certificate in the certificate chain is signed by a trusted organization, also called the Root Certificate Authority (Root CA). Multiple Certificate Authorities branch from the Root CA in a parent-child relationship. An intermediate CA or sub-CA is the subordinate to another CA and issues certificates to other CAs in the CA hierarchy. Issuing CA or a Certificate Service Provider (CSP) is the CA that issue certificates to users for accessing the various e-government services (Hunt, 2001a).

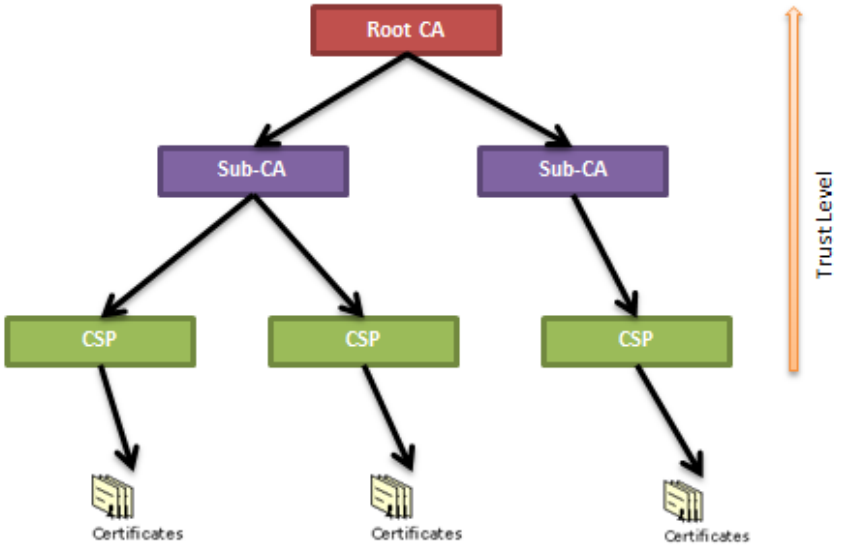

Figure 14: Certificate hierarchy in PKI

PKIOverheid is the PKI designed for trustworthy electronic communication within and with the Dutch government. Using PKI certificates, ensures that the information send over the internet has a high level of reliability (Logius, 2015l). A national PKI certificate hierarchy has been realized to ensure the trust chain we mentioned earlier. The national hierarchy consists of one root and two domains (sub-CAs) each having Certificate Service Providers (CSPs) below them (Logius, 2015m). Each CSP can issue several types of certificates for authentication, encryption, and non-repudiation. The CSPs of the PKI are external agencies who are allowed to issue certificates on behalf of the PKIOverheid. In addition to issuing of certificates, the CSPs also perform the validation and revocation of certificates. This is enabled using a Certificate Revocation List (CRL). It is a publicly accessible list of withdrawn certificates. The users can ensure the validity of the certificates online in a system-to-system manner using the Online Certificate Status Protocol. Therefore the CSPs must ensure that the CRLs are available via an online facility (Bharosa et al., 2015; Hunt, 2001a)

The CSPs affiliated with PKIOverheid have CSP certificates, which allow them to issue certificates. CSP KPN Corporate Market (formerly Getronics), ESG The Electronic Signature B.V., QuoVadis Trust Link B.V., and Digidentity B.V. are the four commercial CSPs who sell PKIOverheid certificates (Logius, 2015o). DigiNotar B.V. was also a CSP who issued PKIOverheid certificates for the Dutch government. A very high profile security incident associated with the digital certificates issued by DigiNotar led to the first digital certificate disaster in the Netherlands (Meulen, 2013).

The DigiNotar Incident

The DigiNotar incident was a high profile security breach related to CAs and PKI in the Netherlands. It affected many private and public organizations and had a huge impact on the e-government infrastructure of the Netherlands. It is therefore necessary to mention the incident here as we will discuss the incident many times in the later chapters of this report.

In the summer of 2011, a major hacking incident in the Netherlands caused a lot of confusion and public attention. In June and July of that year, a hacker accessed the computer systems of DigiNotar B.V. DigiNotar was a company that provided digital certificate services and hosted a number of Certificate Authorities (CAs). Certificates issued included SSL certificates, Qualified certificates, and 'PKIOverheid' (Government accredited) certificates (Prins, 2011). In the interim report (Prins, 2011), published by Fox-IT after an initial investigation in September 2011, it was revealed that the hacker had succeeded in generating and issuing fraudulent certificates. The data of private individuals and companies were at risk of being intercepted and misused. The audit by Fox-IT, following the breach revealed that DigiNotar didn't uncover the breach until mid-July, even though the breach happened in early June. It was also revealed that DigiNotar lacked basic security safeguards, such as strong passwords, anti-virus protection, and up-to-date software patches. Browser makers like Google, Mozilla, and Microsoft permanently blocked all digital certificates issued by DigiNotar, suggesting a complete loss of trust in the integrity of its service. The MinBZK also announced that the security of their websites were not guaranteed and urged the public not to use their websites until new certificates were obtained from other issuing authorities. DigiNotar voluntarily filed for bankruptcy on September 20, 2011 due to the failure of its core business of providing trust through its delivery of digital certificates (Meulen, 2013).

4.4. Summary

In this chapter we discussed Digipoort, an e-government infrastructure for business enterprises provided by the Dutch government and managed by Logius. We introduced the two types of Digipoort – Digipoort OTP and Digipoort PI. In Section 4.1 we discussed the various services provided by Digipoort OTP to different government agencies and businesses. Subsequently, we developed a set of use cases for the Digipoort OTP service to Douane. From the use cases we visualized the interaction of actors like the reporting parties (businesses and intermediaries), government agencies, Vendors, and TTPs with the Digipoort system. Further we also discussed Digipoort PI in Section 4.2, and detailed the infrastructure and services provided by Digipoort PI. Digipoort PI makes use of web services and interface standards to transfer information between businesses and governments. Both Digipoort OTP and Digipoort PI use digital certificates and the PKI to authenticate the users who connect to Digipoort. We also realized the importance of PKI in ensuring the security of e-government services and described the various components of PKI like digital certificates, CSPs, the certificate hierarchy and the CRLs in Section 4.3. A comparison of Digipoort OTP and Digipoort PI has been shown in Table 24 in Appendix I.

In Chapter 3 and Chapter 4 we answered the second sub-question, "*What are e-government infrastructures for businesses?*" First we discussed e-governments in general in Chapter 3. The increasing complexity of e-government implementations enhance the need to focus on security, and therefore justify the importance of understanding the threat landscape of e-government infrastructures. Businesses use e-governments as an infrastructure to submit legally obligated information and also as an online marketplace. Digipoort is such an e-government infrastructure used by businesses. PKI and digital certificates enable the security of e-government infrastructures. However, the DigiNotar incident associated with the Dutch PKI showed that enabling technologies like digital certificates that are used to improve the security of electronic infrastructures can also be sources of vulnerabilities in the system.

STATE OF THE ART

5. Threat Assessment Methodologies

In the previous chapters we discussed e-government infrastructure in general and Digipoort which is an e-government infrastructure of the Dutch government used by businesses. In this chapter we survey the threat assessment methodologies for e-government infrastructures and answer the second sub-question. *State of the art* is part of the *Problem Formulation* phase.

SQ 2: *What is the state of the art in threat assessment methodologies for e-government infrastructures?*

Here we compare threat assessment methodologies from literature and determine the most suitable methodology for this research. Before we perform the survey on threat assessment methodologies for e-government infrastructures, we first conceptualize the definition of a threat landscape from literature in Section 5.1. In Section 5.2, the methodology we used in collecting and analyzing literature about threat assessment methodologies from various academic and non-academic databases is discussed. The results of the literature review are discussed in Section 5.3. Further in Section 5.4 we discuss the characteristics and limitations of the TARA methodology which will be used in this research. Subsequently we provide a summary of the chapter in Section 5.5.

5.1. Threat Landscape

As mentioned in the introductory chapter, there are different definitions for a threat landscape. Different researchers define threats differently in literature. In this section, we perform a survey of different threat classifications in literature. A better understanding of what constitutes a threat landscape can be developed from this section.

Threat agent taxonomies helps analysts in forming a coherent picture of the threat landscape and priorities of remediation for organizations and their assets (Casey et al., 2010). Casey et al. (2010), observes that the focus of most studies in threat modeling and risk assessment techniques continues to be on asset or vulnerability analysis, leaving the analysis of threat agents out of scope. The lack of industrial standards or reference definitions of agents as well as the dynamic nature of many threats is a key problem in this regard (Casey et al., 2010). This makes it important to properly define the taxonomy of threat landscape in the beginning of the research. Lindqvist & Jonsson (1997) mentions the following properties needed for the classification of a phenomenon.

- The categories should be mutually exclusive (every specimen should fit in at most one category) and collectively exhaustive (every specimen should fit in at least one category)
- Every category should be accompanied by clear and unambiguous criteria defining what specimens are to be put in that category.
- The taxonomy should be comprehensible and useful not only for experts in security, but also users and administrators with less knowledge and experience of security.
- The terminology of the taxonomy should comply with the established security terminology (something that is not always easy to define).

We can see many classifications of threats by looking into information security literature. For instance, the Microsoft's STRIDE model is a classification of computer security threats. The acronym is created from the initials of the six threat categories - Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. The model describes the threat manifestations as threat categories but do not address the threat agents directly (Zalewski et al., 2013). Farahmand et al. (2005), created a threat taxonomy based on the above properties, for threats to a network system from two points of view (1) Threat agent, and (2) Penetration technique. The authors explain that a threat is manifested by a threat agent using a specific penetration technique to produce an undesired effect on the network. The threat agents were classified into environmental factors (natural disasters, mechanical, electrical equipment failure etc), authorized users (insiders using the system), unauthorized users (anyone who attempts to cause harm to the system). Techniques of penetration were classified into physical, personnel, hardware, software, and procedural. In addition to this, they also included the ISO 7498-2 standard list of security control measures as a third dimension, to counter the threats (Figure 15). Jouini et al. (2014) developed a multi-dimension hybrid threat classification model for information system security, based on the criteria source, agent, motivation, intention, impacts. The models mentioned above were primarily created for information systems. None of the models provide a consistent definition of threat landscapes.

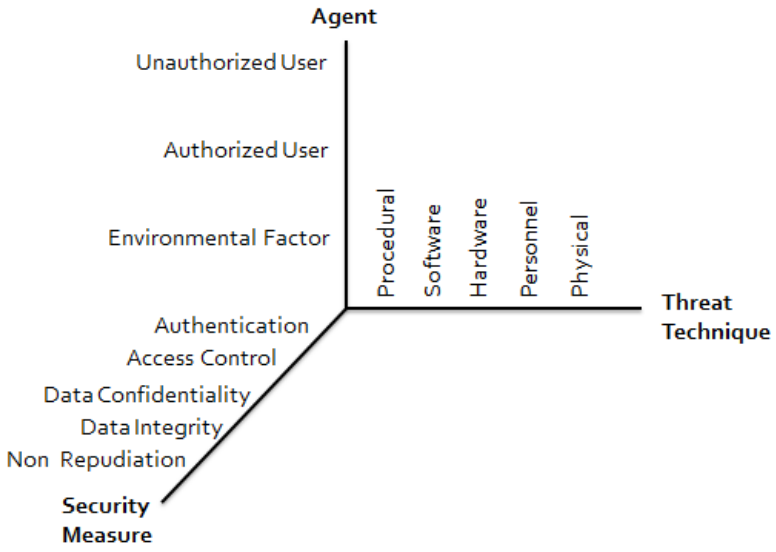

Figure 15: Threat taxonomy by Farahmand et al. (2005)

As seen above, threat agents are an important part of threat taxonomy. Threat agents are also classified in different ways in different literatures. The IBM classification includes "clever outsiders", "knowledgeable insiders" and "funded organizations". Though simple to understand, this classification does not do justice to the widely differing intents, capabilities and access to resources of real world threat agents (Abraham et al., 1991). The Information Security Society of Switzerland (ISSS) describes threat agents, their motivations and their localization. The taxonomy addresses three factors, the identity of the agent, the nature of intent and the place of operations respectively (Ruf et al., 2003). One of the better classifications of threat agent archetypes was developed by Intel. Intel developed a Threat Agent Library (TAL) of 22 agent archetypes, each uniquely defined. The agents are described uniquely

using the attributes like – Intent (hostile/accidental), Access (internal/external), Outcome (threat agent's goal), Limits (legal and ethical limits constraining threat agent), Resource Level (organizational level), Skill level, Objective (attack strategy), Visibility (overt/covert/clandestine). The TAL can improve threat analysis process by providing a consistent library, from which we can select threat agents most relevant to the system under analysis (Casey et al., 2010). In addition to this, Intel also brings in more dimensions to the threat agent using their Methods Objective Library (MOL), which also gives the assessor additional information regarding the methods of the threat agent and the objective it wants to achieve (Rosenquist, 2009). TAL eliminates the need to create a threat library from scratch. It makes the threat assessment process more consistent, faster and repeatable (Casey et al., 2010).

Reflection

The threat taxonomies and threat agent classifications are not standardized, and this leads to different definitions of threat landscapes. From the different classifications of threats we saw earlier, we realized that the threat agents, their attributes, and penetration techniques are important concepts that can be used to define a threat. The results of the analysis are put in the Table 8. According to Mateski et al. (2012) a threat agent can be defined by its attributes. Attributes are characteristics of the threat agent that can uniquely define them (Casey et al., 2010). The threat agent can manifest a threat to an organization and its assets to achieve its objective, using a penetration technique (threat action or method). When developing the threat landscape, it would make much sense to describe, the threat manifestations, the threat agents who cause those manifestations, their attributes and the penetration techniques that can be used by these threat agents. This would make the threat landscape detailed enough to be useful for understanding the threats faced by a system. The system can be an organization, an asset or an infrastructure of the organization.

Table 8: Threat taxonomies

Literature	Threat classification in terms of:
(Farahmand et al., 2005)	Threat agent, penetration method, and security measures
(Jouini et al., 2014)	Source, Threat agent, motivation, Intention, Impact
(Casey et al., 2010; Rosenquist, 2009)	Threat agent, Methods, Objectives

Intel's classification of threat, can be considered as a combination of the concepts defined by (Farahmand et al., 2005) and (Jouini et al., 2014). A conceptual model (Figure 16) can be built using the concepts from the above analysis. The conceptual model shows that the threat to an asset can be defined by three main concepts, the threat agent defined by its attributes, the methods used, and the objectives of the threat agent. The threat agents affect the assets using various manifestations or penetration methods to achieve their objectives. The threat landscape of a system can therefore be understood by studying the threat agents, their attributes, methods, and objectives. These concepts form the cruxes of our research. In the following section the methodology we used for surveying literature about threat assessment methodologies from various academic and non-academic databases is discussed.

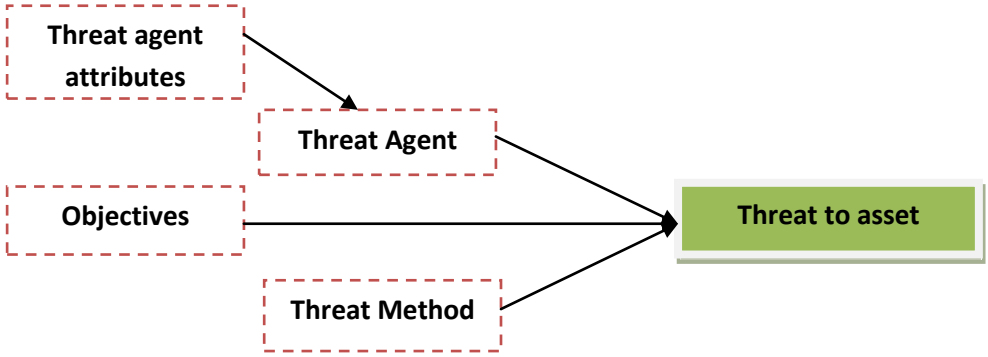

Figure 16: Conceptualization of a threat landscape

5.2. Methodology

We used the following approach to survey the threat assessment methodologies from literature. A search on Scopus with the key words "threat analysis" or "threat assessment", and "egovernment", yielded very few results. To be exact, the search resulted in one study which performed a comprehensive SWOT analysis on the Mongolian tax information system. The same query on Web of Science also did not yield many results. The query was modified using wild card characters to get more results. The query, ((threat* OR threat*assessment) AND e*government) did not yield many results on cyber threat assessment in Scopus or Web of Science. The search on IEEE however revealed a huge amount of literature (more than 14,000), but mostly unrelated to threat analysis or threat modeling. In order get more accurate results, the query was re-modified to (((threat*mod OR threat*analy*) AND e*government AND cyber*). However, this time the number of results returned from IEEE was only 3. The results of the searches points to the lack of dedicated threat analysis research for egovernment infrastructure. In order to get more results on threat assessment methods, the search was made more generic. The key word e*government was removed to ensure a wider view of the various methods for threat analysis. We searched various databases including Scopus, Web of Science, and IEEE using key words like threats, threat analysis, threat assessment and their combinations. Google Scholar was also used to get access to the white papers and technical reports used in the study. Reports that did not exclusively deal with the study of cyber threats were excluded from the analysis.

We analyzed the literature obtained based on the three criteria mentioned below. The three criteria were used to structure the literature analysis and select a suitable threat assessment methodology for our research from the set of threat assessment methodologies we identified in literature.

1) The focus on threat agents – According to Shostack (2014) there are three different types of threat assessment approaches used by assessors depending upon the focus of the threat assessment. They are namely software centric, asset centric and attacker centric methodologies. The software centric approach focuses on the software that is being built or deployed, the asset centric approach focuses on the valuable assets, and the attacker centric approach focuses on the attackers who go after the assets (Shostack, 2014). We defined threat landscape as, the threat agent along with their attributes, the

methods used, and their objectives. Based on our definition of a threat landscape, we need to use a threat agent centric threat assessment methodology to achieve our research objective.

2) Ease of use for non-expert users – This is a non-functional requirement[3] from Logius. Logius managers would like to become familiar with an easy to use methodology, so that it can be used by non-expert assessors in the future. We therefore require a threat assessment methodology that is easy to use for non-expert users.

3) Time constraint in carrying out the assessment – This is a non-functional requirement from Logius with regards to the flexibility and time required to carry out the threat assessment. In addition to the methodology being simple, it should also be flexible and less time consuming to perform.

The three criteria mentioned above are only used to make a systematic selection of threat assessment methodologies from literature, and should not to be confused as design requirements. The findings from the literature are discussed in the following section.

5.3. State of the art – Threat Assessment Methodologies

We analyzed the literature obtained using the methodology discussed in the previous section. The analysis based on the three criteria we discussed earlier - focus on threat agents, ease of use for non-expert users, and time constraint in carrying out the assessment yielded the following results.

Myagmar et al. (2005), describes threat modeling as a step towards addressing the completeness of the system requirements and the security requirements of a system. They describe threat modeling from a requirements engineering perspective and stress the importance of threat modeling for software products and complex systems. Möckel & Abdallah (2010) and Zalewski et al. (2013), uses the Data Flow Diagram tool and Unified Modeling Language (UML) respectively, to characterize the system under investigation and demonstrate the data flows through the system. Myagmar et al. (2005), demonstrates the example of VisFlow-Connect, a Network Traffic Monitoring Tool for characterizing complex systems. The remaining steps in the threat analysis followed by Möckel & Abdallah (2010), Myagmar et al. (2005) and Zalewski et al. (2013) are similar and involve using Microsoft's STRIDE (threat classes) and DREAD (impact calculation of threats) methods for identifying the threats and quantifying the risks associated with these threats respectively. The methodologies used in the papers discussed above follow a technical modeling approach to determine the potential threats to a system. The methodology can be seen as a software centric approach and is dependent on the tools that are used for modeling the system. The approach being technical, does not take into account the various actors involved, and therefore gives a very technical view of the threats. The output of the assessment requires sensible evaluation and interpretation and is therefore difficult to use for non-expert users. The time required to perform the assessment depends on the system under consideration.

[3] Non-functional requirements in Requirements Engineering specify criteria that can be used to judge the operation of a system, rather than specific behaviours (functional behaviours). For e.g. safety, security, flexibility, performance, cost etc (Lamsweerde, 2000).

Vidalis, Jones, & Blyth (2004) devised a Threat Assessment Model for Electronic Payment Systems (TAME) methodology for assessing threats faced by organizations. TAME was developed as a tool that could be used by any computer literate person in any type of organization. The TAME methodology differs from other methodologies by taking into account the organizational and technology issues for comprehensively understanding the threat environment in which the business is operating. Internal and external stakeholders are actively involved in the process. The ultimate goal of TAME is to help the security manager decide how much security is needed and where it is to be applied. TAME is an asset centric methodology and can be performed effectively by a non-expert user. However, the identification of threat agents is unclear and depends on the assessor. It can also be lengthy and time consuming.

The Cyber Threat Susceptibility Assessment (TSA), MITRE (2014), is used to quantitatively assess a system's ability to resist cyber-attack over a range of catalogued attack Tactics, Techniques, and Procedures (TTPs) associated with Advanced Persistent Threat (APT). The TSA process is part of the Mission Assurance Engineering (MAE) methodology, and follows the Crown Jewel Analysis (CJA), which is a pre-requisite to cyber Risk Remediation Analysis (RRA). The methodology is focused especially on APT's, and involves additional steps like CJA and MAE which require considerable system expertise. The methodology focuses on modeling the assets and identifying the threats related to them and is therefore asset centric. The prior knowledge of assets is necessary for using this methodology, and could be difficult for a non-expert user to perform. The time taken depends on the evaluation criteria, and is generally not flexible if the evaluation criteria changes.

	THREAT PROFILE						
	Commitment			Resources			
					Knowledge		
Threat Level	Intensity	Stealth	Time	Technical personnel	Cyber	Kinetic	Access
1	H	H	Years to decades	Hundreds	H	H	H
2	H	H	Years to decades	Tens of tens	M	H	M
3	H	H	Months to years	Tens of tens	H	M	M
4	M	H	Weeks to months	Tens	H	M	M
5	H	M	Weeks to months	Tens	M	M	M
6	M	M	Weeks to months	Ones	M	M	L
7	M	M	Months to years	Tens	L	L	L
8	L	L	Days to weeks	Ones	L	L	L

Figure 17: General Threat Matrix from (Mateski et al., 2012)

Mateski et al. (2012), describes threat metrics and models for characterizing threats consistently and unambiguously. Sandia National Laboratories, the Department of Homeland Security (DHS), the Federal Network Security (FNS) developed the Operational Threat Assessment (OTA) methodology which estimates the current threats faced by a system. The method focuses on characterizing cyber threats using consistent cyber threat metrics and models. The methodology uses a General Threat Matrix (GTM)

to characterize and differentiate threats against targets of interest. The methodology however, does not try to identify the threat agents, and concentrates on building a GTM (Figure 17), using information about the attributes of agents - commitment (includes intensity, stealth, time), and Resources (technical personnel, knowledge, and access). The OTA is designed to provide an efficient threat estimate which is consistent with respect to different organizations and analysts. It reduces the effect of personal bias and preconceived notions of assessors on the results (Mateski et al., 2012). However, threat metrics can be difficult to identify, delimit and quantify. The time taken to perform the assessment depends on the boundary of the system under consideration.

Another methodology, the Intel – Threat Agent Risk Assessment (TARA) was discussed in Casey et al. (2010) and Rosenquist (2009). The predictive output from TARA helps in informed decision making at every level of management, which even non-expert audiences can understand. The methodology applies specifically to Information Security and is an attacker centric (threat agent centric) approach. Casey et al. (2010), expresses the need to focus on threat agents and the use of the Threat Agent Library (TAL) of Intel to perform a more consistent, faster, and repeatable threat modeling process, by focusing only on the most likely threat agents to support the development of optimal security strategies. The lack of research papers based on attacker (threat agent) centric methodologies is however a disadvantage, at the same time it shows that there's a knowledge gap in the use of agent centric threat assessment methodologies for threat assessment in complex systems with multiple stakeholders. TARA and TAL focuses on identifying the threat agents first. A list of threat agents (TAL) exist, which can be adapted to cases to understand the most likely threat vectors. According to Rosenquist (2009), because TARA focuses on the most likely threat vectors it is easy to use and understand. It can also be as quick and simple or as deliberate and complex as needed (Rosenquist, 2009). From this analysis we realize that the TARA methodology's focus on threat agents, its flexibility and its ease of use makes it suitable for this research. TARA is explained in detail in the next section. Table 9 below summarizes the findings from the literature review.

Table 9: Comparison of threat assessment methods

Literature	Methodology	Focus	Expert user needed?	Time constraint
(Myagmar et al., 2005; Zalewski et al., 2013)	Microsoft SDL Threat Modeling Tool	Software	Yes	Depends on the system under analysis
(Vidalis et al., 2004)	Threat Assessment Model for Electronic Payment Systems (TAME)	Asset	No	Time consuming
(MITRE, 2014)	Cyber Threat Susceptibility Assessment (TSA)	Asset	Yes	Depends on the system under analysis
(Mateski et al., 2012)	Operational Threat Assessment (OTA) and General Threat Matrix (GTM)	Threat agent	Yes	Depends on the system under analysis

Literature	Methodology	Focus	Expert user needed?	Time constraint
(Casey et al., 2010; Casey, 2007; Rosenquist, 2009)	Intel – Threat Agent Risk Assessment (TARA)	Threat agent	No	Depends on the prioritization of threats

5.4. TARA

TARA is an information security risk assessment methodology developed by Intel to identify threat agents who are pursuing objectives which are reasonably attainable and can cause unsatisfactory loss to Intel (Rosenquist, 2009). Unlike vulnerability assessments like the Microsoft STRIDE and DREAD methodologies discussed earlier, TARA does not attempt to identify every single weak point. TARA methodology identifies which threat agents pose the greatest risk, their motivation, and the likely methods they will employ. The methods can be cross referenced with existing vulnerabilities and controls to determine the most likely threat scenarios (Rosenquist, 2009). Casey et al. (2010), mentions that mitigation techniques and planning approaches depend on the intent and abilities of the attackers, and that a greater emphasis on analysis from that angle is important. TARA methodology is a step in this direction. The typology of threat agents used in TARA can provide considerable insights into the likelihood and specific nature of the attacks, and can inform the assessor the most suitable and pragmatic mitigation techniques. The following definitions (Table 10) are standard for TARA:

Table 10: Definitions of commonly used terms, adapted from (Rosenquist, 2009)

Terminology	Definition
Vulnerability	Part of information security infrastructure that could represent a weakness to attack in the absence of a control.
Threat agent	Person who originates attacks, either with malice or by accident, taking advantage of vulnerabilities to create loss.
Motivation	Internal reason a threat agent wants to attack.
Objective	What the threat agent hopes to accomplish by the attack.
Method	Process by which a threat agent attempts to exploit a vulnerability to achieve an objective.
Attack	Action of a threat agent to exploit a vulnerability.
Control	Tools, processes, and measures put in place to reduce the risk of loss due to vulnerability.
Exposure	Vulnerability without a control.
Trust Level	The level of trust a threat agent receives from the victim of an attack.

The TARA methodology relies on three main libraries, the Threat Agent Library (TAL), the Common Exposure Library (CEL), and the Methods and Objectives Library (MOL). The CEL library enumerates known information security vulnerabilities and exposures at Intel and is therefore not publicly available due to its confidential nature. In this research, we work around the absence of this artifact by creating sample attack scenarios by the threat agents on the assets. Therefore, a CEL is not created for this

research. We will discuss more about this in the coming sections. The TAL and MOL libraries are explained further.

TAL

The TAL consists of a set of threat agent archetypes defined on the basis of a number of attributes. An important advantage of TAL is that it leaves room to accommodate the evolving threat agents due to changes in economic, political, societal, and technological trends. The TAL library consists of threat agent archetypes (as shown in Figure 18), each uniquely defined by several attributes. The attributes, their descriptions and values are shown in Table 11.

Table 11: Attributes of Threat Agents, adopted from (Casey, 2007)

Attribute Name	Description	Attribute Values
Intent	Defines whether the agent intends to cause harm. Based on the intent, the agent can be hostile or non-hostile.	**-Hostile:** The agent intents to cause harm or inappropriately use assets, and the agent take deliberate actions to achieve that result. **-Non-Hostile:** The agent is friendly and intends to protect the assets, but accidentally or mistakenly takes actions that result in harm.
Access	Defines the extent of agent's access to the company's assets. Based on access, the agent can be internal or external.	**-Internal:** Agent has internal access. **-External:** Agent has only external access.
Outcome	Defines the agent's primary goal.	**-Acquisition/Theft:** Illicit acquisition of valuable assets for resale or extortion in a way that preserves the assets' integrity but damage other items in the process. **-Business Advantage:** Increased ability to compete in a market with a given set of products. The goal is to acquire business processes or assets. **-Damage:** Injury to personnel, physical or electronic assets, or intellectual property. **-Embarrassment:** Public portrayal of organization in an unflattering light, causing Intel to lose influence, credibility, competitiveness, or stock value. **-Technical Advantage:** Illicit improvement of a specific product or production capability. The primary target is to acquire production processes or assets rather than a business process.
Limits	Defines the legal and ethical limits that may constrain the agent.	**-Code of Conduct:** Agents typically follow both the applicable laws and an additional code of conduct accepted within a profession or an exchange of goods or services. **-Legal:** Agents act within the limits of applicable laws. **-Extra-legal, Minor:** Agents may break the law in relatively minor, non-violent ways, such as minor vandalism or trespass. **-Extra-legal, Major:** Agents take no account of the law and may engage in felonious behaviours resulting in significant financial impact or extreme violence.
Resource	Defines the organizational level at	**-Individual:** Resources limited to the average individual,

Attribute Name	Description	Attribute Values
	which the agent typically works. This attribute is related to the Skill level – a specific organizational level implies that the agent has access to at least a specific skill level.	agent acts independently. Minimum skill level: None. **-Club:** Members interact on a social and volunteer basis, often with little personal interest in the specific target. Minimum skill level: Minimal **-Contest:** A short-lived and perhaps anonymous interaction that concludes when the participants have achieved a single goal. Minimum skill: Operational. **-Team:** A formally organized group with a leader typically motivated by a specific goal and organized around that goal. Group persists long term and typically operates within a single geography. Minimum skill level: Operational. **-Organization:** Larger and better resourced than a Team; typically a company. Usually operates in multiple geographies and persists long term. Minimum skill level: Adept. **-Government:** Controls public assets and functions within a jurisdiction; very well resourced and persists long term. Minimum skill level: Adept.
Skill Level	Defines the special training or expertise an agent typically possesses.	**-None:** Has average intelligence and ability and can easily carry out random acts of disruption or destruction but has no expertise or training. **-Minimal:** Can copy and use existing techniques. **-Operational:** Understands underlying technology or methods and can create new attacks within a narrow domain. **-Adept:** Expert in technology and attack methods, and can both apply existing attacks and create new one to greatest advantage.
Objective	Defines the action that the agent intends to take in order to achieve a desired outcome.	**-Copy:** Make a replica of the asset so the agent has simultaneous access to it. **-Destroy:** Destroy the asset, which becomes worthless to the organization or the agent. **-Injure:** Damage the asset which remains in the organization's possession but has limited functionality or value. **-Take:** Gain possession of the asset so that the organization has no access to it. **-Don't Care:** The agent does not have a rational plan, or may make a choice opportunistically at the time of attack.
Visibility	Defines the extent to which the agent intents to conceal or reveal his or her identity.	**-Overt:** The agent deliberately makes the attack and the agent's identity is known before or at the time of execution. **-Covert:** The victim knows about the attack at the time it occurs, or soon after. However the agent of the attacks intends to remain unidentified. **-Clandestine:** The agent intends to keep both the attack and his or her identity secret. **-Don't Care:** The agent does not have a rational plan,

Attribute Name	Description	Attribute Values
		may make a choice opportunistically at the time of attack, or may not place importance on secrecy.
Motivation	Defines what motivates the threat agent to attack.	Refer to Table 12.

The currently available library of threat agents are based on the first eight attributes as shown in Figure 18.

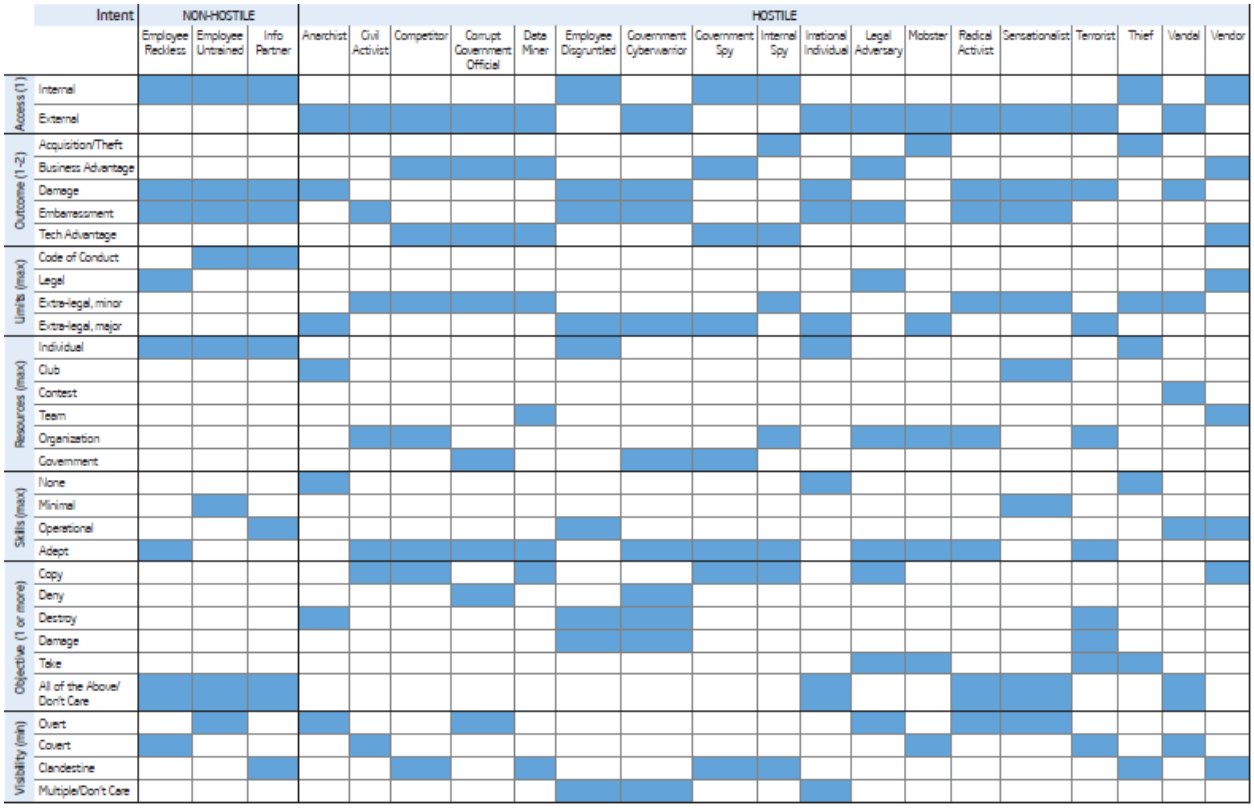

Figure 18: Intel Threat Agent Library, adopted from (Casey, 2007)

Casey (2015) recently added the *Motivation* attribute to the list of attributes of threat agents to define the threat agents more clearly. He defined Motivation as a combination of different types of motivations as shown in Table 12. Casey (2015) defines *Defining Motivation* as the archetypical, single most prevalent and descriptive motivation of the agent archetype, and is used as the basis for a proactive threat agent analysis. According to Casey (2015) the *Defining Motivation* is assigned to all the threat agents and is the only motivation aspect required to define the threat agent. However we also consider *Personal Motivation* to take into account the distinction between organizational and individual motivators. *Personal Motivation* shows the motivation of the individual threat agent - this is especially important in the case of threat agents who act in a group. Personal Motivation allows analysts to consider both the organizational and individual motivators of a threat agent (Casey, 2015).

Table 12: Motivations of threat agents in the TAL, adapted from (Casey, 2015)

Threat agent label	Defining Motivation	Personal Motivation
Employee Reckless	Accidental	--
Employee Untrained	Accidental	--
Information Partner	Accidental	--
Civil Activist	Ideology	Ideology
Radical Activist	Ideology	Ideology
Anarchist	Ideology	Ideology
Competitor	Organizational Gain	Personal Financial Gain
Corrupt Government Official	Personal Financial Gain	Personal Financial Gain
Cybervandal	Dominance	Dominance
Data Miner	Organizational Gain	Personal Financial Gain
Disgruntled Employee	Disgruntlement	Disgruntlement
Government Cyberwarrior	Dominance	Ideology, Personal Financial Gain, Personal Satisfaction
Government Spy	Ideology	Ideology, Personal Financial Gain, Personal Satisfaction
Internal Spy	Personal Financial Gain	Coercion, Ideology, Personal Financial Gain
Irrational Individual	Unpredictable	--
Legal Adversary	Dominance	Personal Financial Gain
Mobster	Organizational Gain	Personal Financial Gain, Coercion
Sensationalist	Notoriety	--
Terrorist	Ideology	Ideology
Thief	Personal Financial Gain	Personal Financial Gain, Personal Satisfaction
Vendor	Organizational Gain	Personal Financial Gain

In addition to the general TAL shown in Figure 18, Houlding et al. (2012) also defined a Threat Agent Library for the Healthcare industry, as shown in Figure 19. We refer to these two TALs while creating the tailored TAL for the e-government domain.

THREAT AGENT ATTRIBUTES		THREAT AGENTS NON-HOSTILE INTENT				THREAT AGENTS HOSTILE INTENT							
		Reckless Healthcare Worker	Distracted Healthcare Worker	Untrained Healthcare Worker	Business Associate	Fraudster	Healthcare Data Thief	Disgruntled Healthcare Worker	Vendor	Radical Activist	Cyber Vandal	Irrational Individual	Curious Healthcare Worker
Access	Internal	■	■	■	■		■	■	■				■
	External					■	■			■	■	■	
Outcome	Acquisition/Theft					■	■						■
	Business Advantage								■				
	Damage	■	■	■	■			■		■	■	■	
	Embarrassment	■	■	■	■			■		■		■	
	Tech Advantage								■				
Limits	Code of Conduct		■	■	■								■
	Legal	■				■	■		■				
	Extra-legal, minor									■	■		
	Extra-legal, major							■				■	
Resources	Individual	■	■	■	■		■	■				■	■
	Club												
	Contest										■		
	Team								■				
	Organization					■				■			
	Government												
Skills	None											■	
	Minimal			■									
	Operational		■		■		■	■	■		■		
	Adept	■				■				■			■
Objective	Copy								■				■
	Deny												
	Destroy							■					
	Damage							■					
	Take					■	■						
	All of the above/Don't Care	■	■	■	■					■	■	■	
Visibility	Overt		■	■						■			
	Covert	■				■	■				■		■
	Clandestine				■				■				
	Multiple/Don't care							■				■	

Figure 19: Threat Agent Library for Healthcare industry, adopted from (Houlding et al., 2012)

MOL

The MOL lists known threat agent objectives – what they want to accomplish, and the most likely methods they employ to reach their objectives. A sample MOL developed by Rosenquist (2009) is shown in Figure 20.

AGENT NAME	ATTACKER					OBJECTIVE		METHOD								IMPACT				
	Access	Trust				Motivation	Goal	Acts					Limits							
		None	Partial Trust	Employee	Administrator			Copy, Expose	Deny, Withhold, Ransom	Destroy, Delete, Render Unavailable	Damage, Alter	Take, Remove	Code of Conduct	Legal	Crimes Against Property	Crimes Against People	Loss of Financial Assets	Business Operations Impact	Loss of Competitive Advantage, Market Share	Legal or Regulatory Exposure	Degradation of Reputation, Image, or Brand
Employee Error	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X		X				X	X	X	X	X
Reckless Employee	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X			X			X	X	X	X	X
Information Partner	Internal		X			Accidental/Mistake	No malicious intent, accidental	X		X	X						X	X	X	X	X
Competitor	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Radical Activist	External	X				Social/Moral Gain	Change Public Opinion or Corporate Policy	X	X	X	X	X				X		X			X
Data Miner	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Vandal	External	X				Personal Gain (Emotional)	Personal Recognition or Satisfaction			X	X				X			X			X
Disgruntled Employee	Internal		X	X	X	Personal Gain (Emotional)	Damage or Destroy Organization		X	X	X				X			X	X		X

Figure 20: Sample MOL library, adopted from (Rosenquist, 2009)

Objectives represent what the threat agent wants to accomplish by attacking the target (Rosenquist, 2009). The likely objectives which threat agents pursue have been mentioned by Rosenquist (2009), as shown in Table 13. In the MOL we will create for e-government infrastructure for businesses in Chapter 5, we will identify the objectives of the threat agents using this classification.

Table 13: Likely threat agent objectives, adapted from (Rosenquist, 2009)

Objective	Example
Theft/Exposure	Exposure of data resulting in loss of competitive advantage, including loss of IP and personal data.
Data Loss	Destruction or alteration of data including corruption, tampering, denial of access, and deletion, in order to make it unusable or decrease its value.
Sabotage	Willful and persistent attempt to cause damage and disruption, including destruction of systems, capabilities, processes, designs, and brand.
Operations Impact	Negative impact on business operations, including manufacturing, engineering, and research.
Embarrassment	Embarrassment targeted at individuals or corporation including real and fabricated defamation, reputation poisoning, and harassment targeting specific personnel or the corporation.
Accidental	No intentional objective to attack.

Methods in the sample library of MOL represent the likely methods through which an attack might occur. The *Limits* of specific agents have already been defined in the TAL. The likely methods used in the MOL are shown in Table 14.

Table 14: Likely methods of threat agents, adapted from (Rosenquist, 2009)

Methods	Examples
Copy, Expose	Copying or exposing intellectual property, information etc.
Deny, Withhold, Ransom	Denying access to the system, withholding, and demanding ransom for freeing the system.
Destroy, Delete, Render Unavailable	Destroy, delete, or make unavailable the system, intellectual property, physical assets, information, or its flow.
Damage, Alter	Damage or alter the system, its components, processes etc.
Take, Remove	Take or remove without permission, physical assets, documents etc.

When the MOL is coupled with the TAL, an assessor will be able to understand the likely attacks on the target system (Rosenquist, 2009). The steps in TARA methodology are shown in Figure 21. There are some limitations that need to be addressed before the TARA methodology can be applied to e-government infrastructure for businesses.

Limitations of TARA

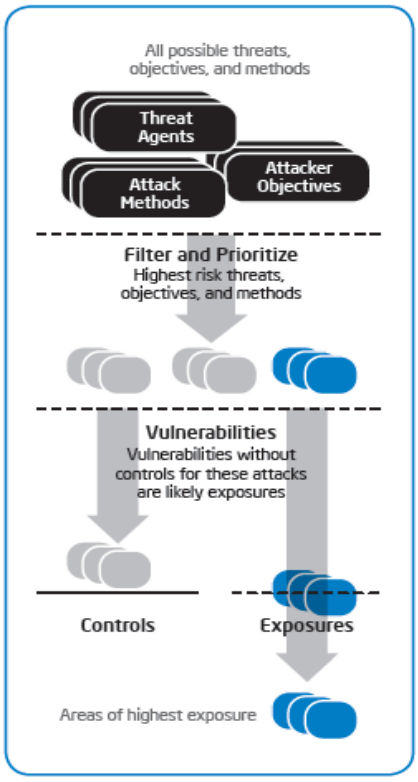

Figure 21: Intel TARA methodology, adopted from (Rosenquist, 2009)

The TARA methodology (shown in Figure 21) can be adopted for this research, with some modifications. Below, we address the two main limitations of TARA.

1) The TAL (Figure 18) was originally made for internal threat analysis at Intel. In order to apply the methodology for e-government infrastructures for businesses, we therefore need to tailor the TAL to include threat agents relevant to e-government infrastructures. This is in line with what Houlding et al. (2012) did while using TARA for healthcare organizations. For instance, the assessors added agents like 'Medical Claims Fraudster' to the list (Figure 19) to account for the healthcare specific agents (Houlding et al., 2012). The limitation of TAL is that it is not an exhaustive library of threat agents that can be applied without modification to every domain.
2) The MOL (Figure 20) is incomplete and is not completely usable in the present format. The MOL shown is suited to Intel's needs. To overcome this limitation, we will need to modify the MOL according to the TAL developed.

By overcoming these two major limitations, it is possible to extend the TARA methodology for e-government infrastructure for businesses and also understand the threat landscape of the Digipoort system under study.

5.5. Summary

We answered the second sub-question, *"What is the state of the art in threat assessment methodologies for e-government infrastructures?"* in this chapter. We conceptualized a threat landscape as the combination of the threat agent, their attributes, methods and objectives as shown in Figure 16. From the state of the art in threat assessment methodologies, we realized that the focus of most studies in threat modeling and risk assessment continues to be on asset or vulnerability analysis, leaving the analysis of threat agents out of scope. Threat analysis based on threat agents is less prominent. The threat taxonomy is not standardized, and this leads to three different themes of threat analysis methodologies. A subset of different software centric, asset centric and threat agent centric methodologies were discussed in the state of the art. Most of the available research is based on software centric threat assessment models, but they are mainly focused on vulnerability analysis during the development lifecycle of softwares. Asset centric methodologies like TAME, take into account the stakeholder's perspective and ensures that the organizational and technology issues are considered for the threat analysis. However, these methodologies can be difficult to execute and are lengthy. The threat agent (attacker) centric methodology of Intel TARA was found suitable for our research because of its focus on threat agents, ease of use and flexibility in adapting to the time constraints of the assessment.

The TARA consists of three libraries the TAL, the CEL and the MOL. The Intel TAL can provide a comprehensive list of threat agent archetypes which can be used as a database of threat agents to select from for the threat analysis. The MOL is used to understand the methods and objectives of the threat agents in the TAL. The CEL will not be used in our research. There are two limitations of the TARA methodology that need to be overcome in order to apply the methodology to e-government infrastructure for businesses. The limitations are related to the incomplete TAL and MOL for e-government infrastructure for businesses. We will discuss in detail about overcoming the limitations of TARA for e-government infrastructure for businesses in Chapter 6, the *BIE* phase of our research.

DESIGN

6. Threat Assessment for E-government

In Chapter 5 we discussed the different threat assessment methodologies with specific focus on threat agent centric approaches. We also discussed the TARA methodology and its limitations. This chapter describes the *BIE* phase of the ADR model. By answering the third sub-question in this chapter, we show how the TARA methodology can be adapted for e-government infrastructure for businesses.

SQ 3: *How can a threat assessment methodology be adapted for e-government infrastructure for businesses?*

In Section 6.1 we describe the motivation for this chapter. This will be followed by a description of the methodology used for tailoring the TAL and MOL in Section 6.2. The results of the tailoring and the tailored TAL and MOL for e-government infrastructures for businesses are described in Section 6.3. We will then summarize the chapter in Section 6.4.

6.1. Motivation

In the previous chapter we discussed two limitations for applying TARA methodology to e-government infrastructure for businesses. We reintroduce the two limitations and discuss the approach to overcome these below.

1) The first limitation is associated with the TAL. The threat agent archetypes defined in the TAL (Figure 18 by Casey (2007) and Figure 19 by Houlding et al. (2012)) can be used in the proactive threat agent risk assessment of an organization. Though all the threat agents defined in that TAL can be likely threats to an organization, some agents are more important from the perspective of e-government infrastructures. In this regard, we need to add the threat agents that are relevant to e-government infrastructure for businesses to the TAL. In other words, we need to tailor a TAL that can be applied for e-government infrastructure for businesses. We tailor the TAL in this chapter.

2) The second limitation is related to the MOL (Figure 20). The MOL is incomplete and is not completely usable in the present format. It is also not suited for e-government infrastructure for businesses. Therefore we need to tailor the MOL for e-government infrastructure for businesses. We tailor the MOL in this chapter.

In the following section, we explain the methodology we used to tailor the TAL and MOL for e-government infrastructure for businesses.

6.2. Methodology

The main objective of this chapter is to tailor the TAL and MOL for e-government infrastructure for businesses. In this section we explain the methodology that is used to achieve this.

6.2.1. Identifying Threat Agents

In order to tailor the TAL for e-government infrastructures we need to identify the threat agents that are relevant for the e-government domain. We identify the threat agents in two steps and then union the identified threat agents to create a tailored TAL. The two steps are discussed below:

1) We look into the use cases of Digipoort OTP in Chapter 4 and identify threat agents that are relevant for e-government infrastructure for businesses. Earlier we discussed several use cases of Digipoort OTP to understand the interaction of the Digipoort system with various actors like reporting parties (businesses and intermediaries), government agencies, vendors, and TTPs. We analyze the use cases to identify threat agents that can be relevant for e-government infrastructure for businesses. These threat agents will become part of our tailored TAL for the e-government infrastructure for businesses.

2) We select a set of threat agents from the TAL library (Figure 18) created by Casey (2007), by analyzing past incidents in the public sector extracted from a publicly available database of incidents. In order to select a subset of threat agents from the above mentioned TAL, we extracted a list of security incidents in the Government/Public sector over the past 5 years (2015 to 2011). A publicly available incident database was used for this purpose. Privacy Rights Clearinghouse, a non-profit consumer education and advocacy project, published a chronology of data breaches since 2005 for various organization types. Figure 22 shows how the sorting function of the database was used to get the list of incidents for the year 2015. Similarly, incident lists for the years up to 2011 can be obtained from the database. We only extracted incidents that provided enough information about the responsible threat agent and with proper references. Based on the information collected online about the incidents, we identify the threat agents involved by comparing them with the already defined threat agent archetypes in the pre-existing TAL (Figure 18).

The breach incidents in the government sector were extracted and put in a tabular format as shown in the Appendix II. The table shows, 1) the incident date, 2) the affected party, 3) a short description of the incident, 4) assets compromised, 5) threat agent involved, 6) the objectives of the threat agent, and 7) the methods of the threat agents. Every threat agent type who is present at least once in the table will be considered in the tailored TAL for the e-government domain. The incident list is an evidence of the past threats. We assume here that a particular threat agent, who has attacked an e-government system in the past, can probably attack similar systems in the future too. It is therefore important to consider these threat agent archetypes in the threat analysis of e-government infrastructures.

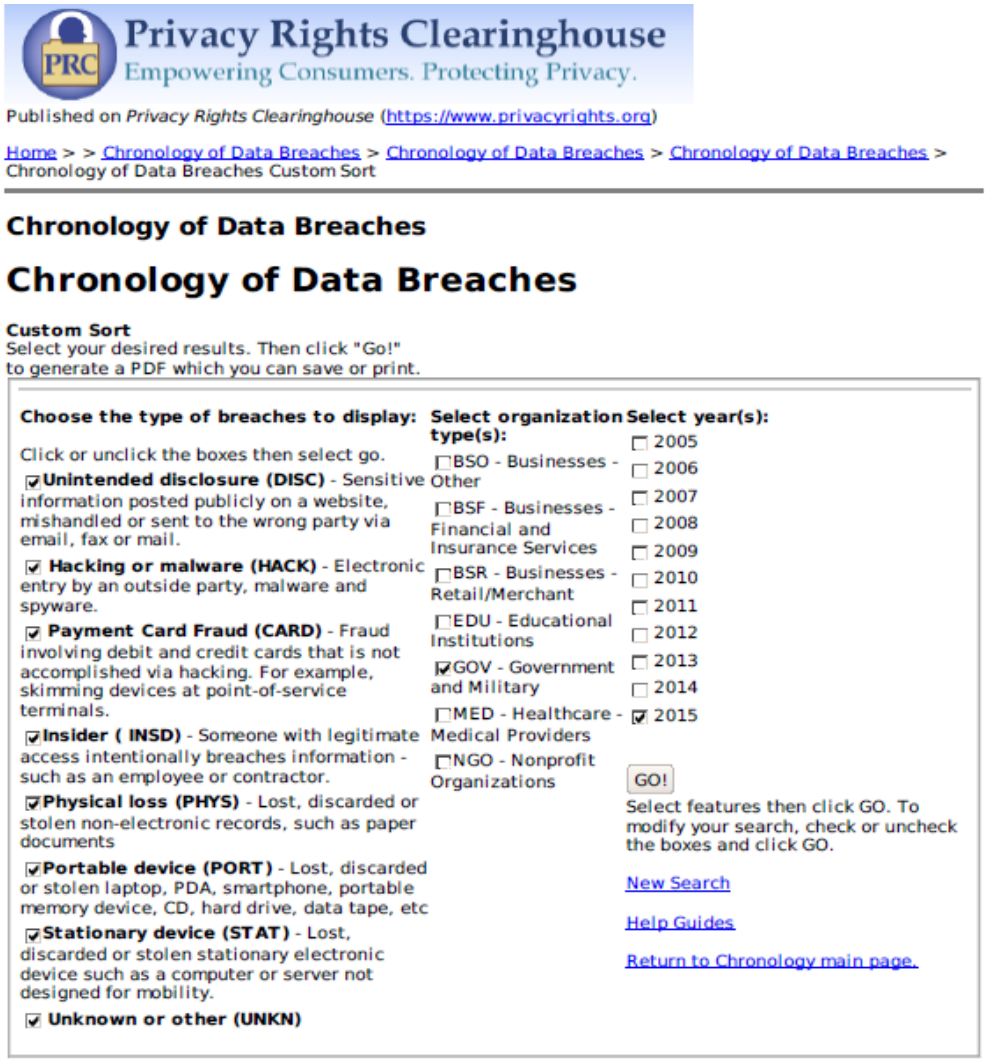

Figure 22: Privacy Rights Clearinghouse database (Privacy Rights Clearinghouse, 2015)

By executing the two steps discussed above and combining their results, we will have a list of threat agents that are relevant for e-government infrastructure for businesses. In the following section we describe the methodology we used to identify the attributes of the threat agents in the tailored TAL.

6.2.2. Identifying Threat Agent Attributes

We identify the attributes of the threat agents using the following steps:

1) Desk research is conducted to identify the attributes from literature. We identify each attribute by analyzing the literature. Information about the various actors collected from academic journals, online information, books etc are used to identify the specific characteristics of each threat agent. The results of the exploratory stage in Chapter 4 about Digipoort OTP are also used for this purpose.

2) We interview two subject matter experts in cyber security risk services and research in the public sector to identify the threat agent attributes that cannot be identified completely from literature. The

interviews in this section to identify the attributes of threat agents and in the next section to identify the methods and objectives of threat agents are executed together. The common interview protocol for the interviews is discussed in Section 6.2.4.

Once we have identified the attributes of the threat agents using the steps mentioned above, we will have a tailored TAL for e-government infrastructures for businesses.

6.2.3. Identifying Threat Agent Methods and Objectives

We use the following steps to understand the *Methods*, *Objectives, and Trust Level* of the threat agents and build an MOL:

1) We use the extracted list of past incidents in the public sector, shown in Appendix II to check for likely methods and objectives of the threat agents. The *Methods*, *Objectives, and Trust Level* are identified from the information obtained about the incidents, and the knowledge from academic journals, white papers, online information, and books related to information security. The *Access*, *Motivation*, and *Limits* of the threat agents are obtained from the tailored TAL we will obtain as a result of the application of the methodology in the previous section.

2) As mentioned in the previous section, we interview two subject matter experts in cyber security risk services and research in the public sector to identify the threat agent methods and objectives that could not be identified completely from literature. The common interview protocol for the interviews is discussed in Section 6.2.4.

6.2.4. Interview Protocol

We administered a structured interview to two subject matter experts in the cyber security risk services and research in the public sector, in order to understand the attributes, methods and objectives of threat agents in the tailored TAL (The identities of interviewees are not revealed to protect confidentiality). The Security Expert 1 we interviewed has more than 20 years of experience as a consultant in Cyber Risk Services, with an in depth knowledge in the domains of security, risk management and IT-architecture. The Security Expert 2 has extensive experience as an analyst in cyber attack research in a public organization. The expert has knowledge on the different types of acts of digital attacks, their developments, trends and capacities of threat agents.

The interview questions are formulated in a way as to understand the attributes, objectives, and methods based on their pre-defined classifications in Table 11, Table 13 and Table 14 respectively. This is the reason behind using a structured interview approach. Most of the questions are associated with the newly added threat agents in the tailored TAL like *End User Reckless, CSP, and Vendor Reckless*. There are also some questions related to the characteristics of already existing threat agents like *Fraudsters* and *Mobster*s. The interview questions were supplemented with options for answers, because we were looking for specific responses from the experts. We also asked the experts to support their judgments with practical examples from their past experience and asked additional questions to clarify unclear responses.

While analyzing the interview responses, we first created the transcripts of interviews for each expert. Then we compared the responses of the experts for each question and tried to find if their responses matched. When there was a disagreement in responses between the experts, we selected a union of their responses and tried to supplement it with evidences from the interviews or from literature wherever possible. Since the experts have different levels of experience, it is possible that they might have had varying levels of interactions with incidents related to the threat agents we questioned about. Therefore a difference in opinion does not point to a mistake in judgment, but to a difference in experiences. We tried to minimize this bias by backing the interviewee responses with evidences from literature. The interview questions and the transcripts of interviews are shown in Appendix III.

6.3. Results

In this section we describe the results obtained after tailoring the TAL and MOL for e-government infrastructure for businesses according to the methodology discussed in the previous section. In Section 6.3.1 we describe the threat agents we identified as relevant for e-government infrastructure for businesses. In Section 6.3.2 we discuss the attributes, methods and objectives of the threat agents we identified as a result of the application of the methodology in sections 6.2.2 and 6.2.3. The tailored TAL and MOL for e-government infrastructure for businesses are shown in Section 6.3.3.

6.3.1. Threat Agents Identified

In this section we describe the threat agents we identified using the methodology described in Section 6.2.1. In Section 6.3.1.1 we describe the threat agents that are relevant for e-government infrastructures for businesses identified from the use cases of Digipoort OTP. Further, in Section 6.3.1.2 we describe the threat agents we identified from the past incidents in the public sector.

6.3.1.1. Threat Agents from Digipoort OTP Use Cases

In Chapter 4 we discussed several use cases of Digipoort OTP. In the use cases, we presented how the Digipoort system transfers messages between the businesses and the governments. We also described the interaction of other actors like Certificate Service Providers (CSPs) and Vendors with the Digipoort system. Based on the use cases and the information obtained from the architects and managers of Digipoort OTP in Logius, the following actors were identified as probable threat agents that could be added to the TAL in order to tailor it for e-government infrastructure for businesses.

End Users

The use cases of Digipoort OTP show the interaction of end users with the Digipoort system. Both businesses and government agencies can be considered as end users of Digipoort. The intermediaries or HUB's which help businesses connect to the Digipoort system can also be considered under this category, because they perform similar actions on the system and are expected to have attributes similar to those of an end user.

(Bleikertz et al., 2013) in their cloud system model, identifies customer as a possible threat agent. In this report we will look at both customers who act with a hostile and a non-hostile intent as possible threat agents. Non-hostile customers can be a threat due to their carelessness (Ostrich attitude) or lack of

training (charlatan attitude) (Bleikertz et al., 2013). On the other hand customers who act in a hostile manner to Digipoort OTP can be considered as trying to perform fraud with the data since the Digipoort handles information like financial reporting that are especially susceptible to fraud. According to a survey conducted by K.P.M.G in 2007, fraudulent financial reporting ranks as the second most common fraudulent activity in organizations (KPMG, 2011). We therefore consider the hostile customers here as Fraudsters. The two end user threat agent archetypes are mentioned below. We will discuss the end user threat agent in detail in the Section 6.3.2.

- *End-user Reckless (non-hostile)*

  They are users of the system who could cause unintentional damage to the system, due to their reckless behavior or carelessness.

- *End-user (hostile) or Fraudster*

  They are users of the system who intentionally attempts to access the information in the system, to perform fraud.

Trusted Third Parties

Trusted Third Parties or Certificate Service Providers (CSPs) represent the third parties that help the customers send messages using the PKI. Earlier we also discussed a major security incident related to a CSP (DigiNotar) in the Netherlands that led to a major realization regarding the threats CSPs pose to digital certificate based authentication in IT infrastructures. CSPs provide end users with certificates to access the Digipoort system and are a major part of many e-government infrastructures.

- *Certificate Service Providers (non-hostile)*

  They are third party certificate providers for the Public Key Infrastructure (PKI). Non-trustworthy Certificate Service Providers can have a big impact on the Digipoort system as seen in the Diginotar incident.

Vendors

This group represents the service providers who have service level agreements with Logius, in order to provide important services to Digipoort. In the case of Digipoort OTP, the vendor plays a very important role, as everything from building to maintenance of the system is being done by the vendor. This is clearly demonstrated in the use case in Figure 10. The TAL (Figure 18) developed by Casey (2007) enumerates vendors as a hostile actor and has already defined its attributes. Casey (2007) however did not mention the possibility of vendors being a non-hostile threat agent. Due to the high interdependency of e-government infrastructures on the vendors, we should also consider vendor as a threat agent for their non-hostile actions. Moreover, E-government outsourcing is widely applied among many developed countries because of the cost effectiveness, availability of technical skills and qualified personnel from vendors (Yang, Li, & Zuo, 2008). This makes it even more important to consider the non-hostile actions of a vendor as a likely source of threat for e-government infrastructures. We will describe both the hostile and non-hostile Vendor threat agent in detail in the Section 6.3.2.

- *Vendor Reckless (Non-hostile)*

They are service providers of e-government infrastructures with internal access, and acting in a reckless or careless manner. Because of their internal access and familiarity of the infrastructure their reckless actions can lead to many effects on the e-government infrastructure. We have discussed in detail about the effects of vendor recklessness on the e-government infrastructure in Section 6.3.2.3.

Please note that, *Vendor (Hostile)* was already defined by Casey (2007) as the business partner who seeks inside information for financial advantage over competitors, and is therefore not mentioned here as a threat agent we identified from the Digipoort OTP use cases. In the following section we discuss the threat agents we identified from past incidents in the public sector.

6.3.1.2. Threat Agents from Past Incidents in Public Sector

We mentioned in Section 6.2.1 the methodology for identifying threat agents from past incidents in the public sector. Based on our analysis, the following threat agent archetypes (Table 15) from the TAL (Figure 18) appear in the incidents list (Appendix II) at least once. The actors which were identified in the section above from Digipoort OTP use cases – *End Users Reckless, Fraudsters, Certificate Service Providers, and Vendor Reckless*, together with the threat agents in Table 15 will give us a tailored TAL for e-government infrastructure for businesses.

Table 15: Threat agents identified from past incidents

Threat agent label	**Access (Internal/External)**	**Assets compromised**	**Common tactics** (Casey, 2007)
Civil Activist	External	Databases, websites, network	Electronic or physical business disruption; theft of business data.
Foreign Government Spy[4]	External	Network, information	Theft of IP or business data.
Mobster	External	Information	Theft of IP, Personally Identifiable Information (PII), or business data; violence.
Employee Disgruntled	Internal	Information	Abuse of privileges for sabotage, cyber or physical.
Internal Spy	Internal	Information	Theft of IP, PII, or business data.
Thief	Internal/External	Information, hardware	Theft of hardware goods or IP, PII, or business data.
Vendor (Hostile)	Internal	Documents and information	Theft of IP or business data
Employee Reckless	Internal	Information	Benign shortcuts and misuse of authorizations.
Employee Untrained/Employee Error	Internal	Information	Poor process, unforeseen mistakes, avoidable errors.

[4] This threat agent has attributes similar to that of the *Government Spy* actor in the TAL, except for the access which is *External* for the threat agent found from the incidents list, and *Internal* for the *Government Spy*.

Caveats of Past Incident Data Analysis

The methodology used for identification of threat agents from past incidents are not without caveats. Below we reflect on the major caveats associated with the selection methodology for threat agents from past incidents.

1) We analyzed around 172 incidents in the public sector from a period of April 2015 to February 2011. In the incident list in Appendix II, we have listed 47 incidents from the 172 incidents analyzed. We had to exclude around 125 incidents from the list due to lack of proper evidence about the threat agents. This is mainly attributed to the lack of clarity about the threat agent from the incident data, insufficient information about the incident and the lack of proper evidence about the incidents (references). Around 28 incidents mentioned the term *hacker* but did not support it with information regarding the objectives or motivations of the hacker. We were therefore unable to adjudge the hackers to a specific threat agent archetype. Around 8 incidents were reported due to software or system error. We ignored these incidents from our analysis because system errors do not fall in the scope of our study. The remaining 89 incidents were excluded because they did not show any conclusive evidence that could link them to a particular threat agent in the TAL in Figure 18. The quality of incident information available might have acted as a moderating variable in our selection of threat agents. However, we tried to minimize this bias by supporting the incident data with information from additional sources wherever possible.

2) The Privacy Rights Clearinghouse chronology of data breaches only deals with incidents in the government and military sector of the United States of America. However, due to the fact that cyber security is an increasingly complex global issue, similar incidents can also be applicable to the governments of other nations in the world (UN, 2011). Therefore we assume in this research that the Privacy Rights Clearinghouse chronology of data breaches is representative of the incidents happening in the public sector in general.

3) Databases similar to the Privacy Rights Clearinghouse are not readily available, have a distinctive vocabulary, or are difficult to use. For instance the VERIS Community Database (VCDB) is an open and free repository of publicly-reported security incidents in VERIS format. The Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner (Verizon, 2015b). However it is difficult to adopt such a vocabulary for this particular research due to the differences in definitions of concepts used in the research and VERIS. Therefore we assume that the Privacy Rights Clearinghouse chronology of data breaches is the most suitable incident list that can be used for this research.

4) The published chronologies of data breaches might not be exhaustive and could have undergone changes after the snapshot of incidents were taken from it. However, a cross sectional data collection is the only feasible approach in this circumstance.

6.3.2. Threat Agents – Attributes, Methods & Objectives

In this section, we discuss the attributes, *Methods*, *Objectives*, and *Trust Level* of the threat agents that we identified in Section 6.3.1. As seen in Section 5.4, each threat agent in the TAL is defined by nine

attributes. They are *Intent, Access, Outcome, Limits, Resource, Skill Level, Objective, Visibility, and Motivation* as shown in Table 11. We also discussed the classification of likely *Objectives* and *Methods* of threat agents in Table 13 and Table 14 respectively in Section 5.4. We applied the methodology we discussed in Section 6.2.2 for identifying the attributes of threat agents and the methodology in Section 6.2.3 for identifying the methods, objectives, and trust level of threat agents. The results are discussed below per threat agent. We first discuss the attributes of the threat agent and then discuss the *Trust Level, Methods,* and *Objectives* of that threat agent. All the attributes of each threat agent are summarized in the tailored TAL in Figure 23, and the *Methods*, *Objectives*, and *Trust Level* of threat agents are summarized in the tailored MOL in Figure 24.

6.3.2.1. End User

In Section 6.3.1.1 we identified the end users of Digipoort OTP as a possible threat agent, mainly in two ways – unintentional damage due to reckless behaviour, and intentional damage by performing fraud. We discuss the attributes, *Trust Level, Methods* and *Objectives* of these two threat agent types in this section.

A user of Digipoort can be either,
1) The businesses that directly connect to Digipoort or,
2) The intermediaries or HUB's that connect to Digipoort on behalf of the businesses.

We therefore use *End User* as a common term to identify both types of users. Cotterman & Kumar (1989) defined end user as any organizational unit or person who has an interaction with the computer-based information system as a consumer or producer/consumer of information. With respect to Digipoort, both businesses (and intermediaries) which send information to Digipoort and receive status messages from the government agencies, and the government agencies which receive information from businesses (and intermediaries) and send status messages to businesses (and intermediaries) are end users. For our analysis, however we only consider end users on the business side in order to make a clearer classification of the agent.

TAL Attributes

We discuss the attributes of the two *End User* threat agent archetypes here. We first discuss the attributes that are common for a reckless end user and fraudster together and then discuss the remaining attributes separately. The attributes of *End User Reckless* and *Fraudster* threat agents have been summarized in the tailored TAL in Figure 23.

Stanton et al. (2005) researched the beneficial and detrimental behaviors of information technology users within organizations that lead to information security related problems. Those individuals possess substantial internal access to the information assets of the organization. However the End User threat agents in question here do not enjoy the benefits of internal access to the Digipoort system, nor are they individuals. They are not insiders, but external actors who access the system for the purpose of exchanging messages. With this regard, their ***Access*** attribute is limited to being *External*. Moreover, the resources available for the agent are pertaining to that of an organization. The attribute, ***Resources*** will therefore be *Organization*, with a minimum ***Skill*** level of being *Adept* (Casey, 2007). Typically, for the

government side end users whom we omitted from this analysis, the *Resources* attribute will be *Government.* Stanton et al. (2005) observed that the intentions of users could be malicious, neutral, or beneficial. Since we are considering end users as a possible threat, and since the ***Intent*** attribute in the TAL is defined dichotomously as *Hostile/Non-Hostile*, we will leave the beneficial intentions of the end user out of this analysis. In line with that observation, for the attribute *Intent,* both *Non-Hostile* and *Hostile* actions of the end users need to be considered.

- *End User Reckless*

  Furnell (2005) stresses the importance of security within end user systems and applications. He mentions that adequate protection is not achieved by default, and the reason for lack of adequate security in some cases can be blamed on careless or irresponsible end-users. He also points out that the underlying unfriendly nature of a technology can be a significant factor in end user misuse. At the client layer, users can cause harm by introducing errors or by accessing systems without authorization (Laudon & Jane, 2012). Careless errors could be in the form of misplacing a crucial document (physical or electronic), using a very weak password, writing down passwords, or leaving a secure system unattended (Fisher, Tinsley, & Strader, 2009). Bottom (2000) mentions in his article that errors could occur when an actor behaves recklessly. In this report, we will consider careless mistakes, a result of reckless behavior.

  An end user with non-hostile intent might not break the law, and is usually bounded by a contract. However a reckless end user might not follow the code of conduct normally associated with the use of information systems. Casey (2007) has already described a reckless employee as behaving within the applicable laws, but not following a suitable code of conduct. A reckless end user can also be set similar values for the *Limits* attribute. An end user, by being reckless deliberately circumvents safeguards for practicality, but do not break any laws in the process (Casey, 2007). They are however not acting within the code of conduct that should be followed by the end users. In the case of Digipoort, end users are required to agree to certain terms of use with Logius, before they can connect to Digipoort. Reckless behaviour might violate some of these terms of use, but they act within the limits of applicable laws. The ***Limits*** attribute is therefore set as *Legal*. Similarly, the ***Visibility*** attribute of a reckless end user can be *Covert*. Since the actions of a reckless end user are not within the acceptable codes of conduct, the end user might be more inclined to be covert about his actions rather than be open about it.

  Being a non-hostile agent, the objectives of a reckless end user do not fall in any category that is associated with an intentional attacker. The agent does not have a rational plan and do not have a clear objective. Like all the other *non-hostile* agents defined in the TAL, the ***Objective*** attribute can be considered as *All of the above/Don't care.* Also, with the intent being non-hostile, the ***Motivation*** of the careless end user can be considered to be *accidental* (Casey, 2015). The outcome attribute defines an agent's primary goal, or what they hope to accomplish with an attack. A reckless user does not have a definite goal because they do not attack intentionally. Their actions could however cause damage and reputation loss to the organization (Casey, 2007). The ***Outcome*** attribute is therefore, *Damage* and *Embarrassment*.

- *Fraudsters*

  During the exploratory analysis about Digipoort OTP at Logius, a Fraud Risk Manager mentioned that hostile actions against the Douane could be perpetrated to acquire information for smuggling goods through the ports. An instance where organized crime groups managed to access secure data about containers from port companies in Antwerp is an example worthy of supporting that claim (Bateman, 2013). Though this attack was perpetrated by organized crime groups with the hired help of hackers from Belgium, hostile actions like these could also be conducted by fraudulent end users. Houlding, Casey, & Rosenquist (2012), created a threat agent library for the healthcare industry as shown in Figure 19, in which they defined the main attributes of an agent performing fraudulent activities. Their construction of the *Fraudster* agent will be reused here as an umbrella term for actors which exhibit fraudulent behavior, including the fraudulent end user. Subsequently we also reuse their definition of the attributes of *Fraudsters*, except for the *Motivation* attribute which they did not define in their TAL.

  We discuss the ***Motivation*** attribute of a Fraudster here. Organizational climate is an important factor that might lead to employees carrying out fraud. For example, employees of an organization might be more interested in committing fraud if it furthers the interest of the organization (Murphy & Dacin, 2011). *Organizational Gain* can therefore be considered as an important motivation of the *Fraudster* threat agent. Croall (1992) classifies Fraud under the list of White-collar crimes. Holtfreter (2005) mentions that corporate crime (committed with the support of the organization) literature identified profit maximization as a key motivating factor in white-collar crime. Casey (2015) mentions that in the case of an organizational threat agent, it is also important to take into consideration the motivation of an individual working for that organization. *Personal Financial Gain* can motivate individuals working for an organizational threat agent. Murphy & Dacin (2011), mentions that the motivation of a fraudster could be financial, pressure (e.g. pressure to retain a position), or social (e.g. desire to retain or gain respect or enhance their self-esteem and status). When asked about the most likely personal motivation for fraudsters, the security experts we interviewed replied that while social pressures are important, the most likely personal motivation is indeed *Personal Financial Gain*. The Motivations for a Fraudster can therefore be both *Organizational Gain* and *Personal Financial Gain*. The excerpts from the interviews are shown in Appendix III.

Methods & Objectives

We discuss the *Methods* and *Objectives* of the two End User threat agent archetypes here. The *Methods* and *Objectives* of End User Reckless and Fraudster threat agents have been summarized in the tailored MOL shown in Figure 24. As an end user of the system, the businesses and intermediaries which use Digipoort are partially trusted by Logius. This can be posited considering the fact that there's a well-defined connection manual and connection process for users to connect to Digipoort. In addition to that, the users are expected to act within the terms of use put forward by Logius (Logius, 2015c). Similarly, end users generally have agreements with the owners of the system in order to act in a certain manner. The end users therefore enjoy a partial trust from the owners of the system. The ***Trust level*** of End Users is therefore *Partial.*

- *End User Reckless*

  The motivation of a reckless end user as identified earlier is *Accidental*. A reckless end user does not have a malicious intent as its ***Objective***. However even with a non-malicious intent there can be negative effects on the infrastructure due to their reckless actions. For instance, the reckless use of the system could lead to data loss, and/or operations impact (from Table 13). It is therefore important to identify the effects on the infrastructure due to their reckless behaviour. In order to understand the effects of reckless use of the e-government infrastructures by end users, we asked security experts as shown in Appendix III. The experts agreed that a reckless end user can cause *Theft/Exposure, Data Loss, Sabotage, Operations Impact* and *Embarrassment*. One expert opined that sabotage was not often seen as an effect of reckless end use. Therefore we consider the most likely effects of reckless end use by end users as *Theft/Exposure, Data Loss, Sabotage, Operations Impact and Embarrassment*.

  Reckless behavior like misuse of certificates can lead to copying or exposure, and lead to unavailability of the information flow between the businesses and the governments (Zeltser, 2015). The security experts agreed that the most likely method of attack due to reckless end use is copying or exposure of information. One expert also mentioned that recklessness in the use of a system by end users can make the system unavailable in many cases. We therefore consider the most likely ***Methods*** of attack as *Copy/Expose* and *Destroy, Delete, Render Unavailable*.

- *Fraudster*

  As mentioned earlier, the most defining motivations of Fraudsters are *Organizational Gain* and *Personal Financial Gain*. Considering that the fraudsters are motivated by organizational and/or personal financial gain, the objective of fraudsters could be theft or exposure of valuable information. The security experts we interviewed confirmed that the most likely ***Objective*** of a Fraudster can indeed be *Theft/Exposure* of information. They cited stealing of access codes, and tax information by Fraudsters as most common examples of this objective. The security experts also mentioned that copying or exposure of information was the most likely method employed by Fraudsters to achieve their objectives. We therefore set the most likely ***Methods*** of Fraudsters as *Copy/Expose*.

6.3.2.2. Certificate Service Provider (CSP)

In Section 6.3.1.1 we defined CSPs of the PKI as a possible threat agent for e-government infrastructures. The use of PKI and the importance of CSPs in an e-government infrastructure were discussed in Section 4.3. We discuss the attributes, *Trust Level, Methods* and *Objectives* of CSPs as threat agents in this section.

TAL Attributes

We have summarized all the attributes of a CSP threat agent in the tailored TAL in Figure 23. As discussed in Section 4.3, the DigiNotar incident is a clear example of how CSPs can be a threat to the information systems of individuals and organizations. DigiNotar issued PKIOverheid certificates which were used in the working of the PKI of the Dutch government. The e-government infrastructure services

of the Dutch government were affected by the Diginotar incident as the PKIOverheid certificates had to be revoked and reissued by a new CSP after the Diginotar incident (Meulen, 2013; Networking4all, 2011). As shown in the use case diagrams in Section 4.1.2, the CSPs enable the authentication of end users, before an end user can send a message over the SMTP – MSA interface. In the DigiNotar incident, the actions of DigiNotar (the firm) were not hostile. Their negligence in employing basic security safeguards resulted in the extensive compromise. The lack of basic security controls like an anti-virus software, and failure to update and patch software installed on the public web servers were the primary reasons for the vulnerability (Meulen, 2013). It was facilitated in part by the company's network segmentation and firewall configuration (Hoogstraaten et al., 2012). They were involuntarily acting as a springboard for attack on their customers. The ***Intent*** attribute of the agent can therefore be considered as *Non-Hostile.*

Businesses or intermediaries who wish to send information through Digipoort buy certificates from CSPs, which is then used to make a secure connection to Digipoort. The CSP is therefore a service provider who does not have internal access to the Digipoort system. The ***Access*** attribute can therefore be considered as *External*. A CSP in the national PKI hierarchy needs to be compliant with ETSI TS 101 456 (European specification for qualified certificates) and additional governmental PKI requirements contained in the Programme of Requirements (Logius, 2015m). The Programme of Requirements contains standards of reliability and quality of service, the formats of certificates and Certificate Revocation List's and the procedures followed when an organization as a certification service provider (CSP) will join the PKI for the government (Logius, 2015n). The actions of the CSP are therefore bounded by standards, in addition to laws of the state. The ***Limits*** attribute will therefore be *Code of Conduct.*

The ***Resources*** attribute will be *Organization*, considering that CSPs are organizations. These organizations are highly skilled, as they are required to maintain a very complex certification mechanism. They are therefore *Adept* in the ***Skills*** attribute. Similar to the end user defined earlier, and like all the other *non-hostile* agents defined in the TAL, the ***Objective*** attribute can be considered as *All of the above/Don't care,* because there is no rational plan executed by the CSP. Also, with the intent being non-hostile, the ***Motivation*** of the erring CSP can be considered to be *accidental* (Casey, 2015). Even though the intention is non-hostile and motivation is accidental, a compromised certificate can cause damage and reputation loss to the organization (Casey, 2007). The ***Outcome*** attribute is therefore, *Damage* and *Embarrassment*.

The ***Visibility*** attribute represent the intention level of an agent to conceal or reveal his or her identity (Casey, 2007). The breach in the DigiNotar systems was detected by DigiNotar in mid-June. DigiNotar tried to contain the breach and did not reveal the system compromise until end of August, when the contents of a rogue wild card certificate for google.com was posted publicly online. The unrevoked rogue certificate was abused on a large scale, leading to Man-In-The-Middle (MITM) attacks on approximately 300,000 users located in the Islamic Republic of Iran (Hoogstraaten et al., 2012). An intention to conceal the attack on the organization and its customers is seen here. This could have been due to the high stakes involved. The business of a CSP is based on the trust the root CA and the customers place on it. Revealing a system breach could lead to loss of trust among the certificate chain and the customers. This can have a negative impact on the CSP's business. It is therefore clear that a CSP

can be clandestine in concealing any misuse due to errors in their systems or processes. The attribute *Visibility*, can thus be considered as *Clandestine.*

Methods & Objectives

The *Methods* and *Objectives* of CSPs have been summarized in the tailored MOL shown in Figure 24. Being a part of the PKI, the CSPs are subject to strict standards and processes to maintain the trust in the certificate hierarchy (Bharosa et al., 2015). We can therefore consider that the CSPs are partially trusted by the government organizations. The ***Trust level*** is therefore *Partial*.

As a threat agent, their motivations are accidental and they do not have a malicious ***Objective***. Their non-malicious objectives can however have negative effects on the target infrastructure and organization. We noticed from the DigiNotar incident that *Data Loss* can be a likely effect of such an incident. For instance, during the DigiNotar incident, the email and other services of Google for several users were intercepted by the DigiNotar attacker. This gave the attacker, not only access to the emails, but also the opportunity to reset passwords for other applications used by the users (Prins, 2011). In addition to this, the affected organizations were impacted operationally because they had to completely replace the compromised digital certificates (Meulen, 2013). When we asked the security experts about these effects, they mentioned that *Data Loss*, *Operations Impact* and *Embarrassment* are the most likely effects of an incompetent CSP.

The errors or compromises made by a CSP can make the e-government infrastructure vulnerable. It can lead to forgery or duplication of keys for malicious intent, by other malicious actors (Hong et al., 2012). The methods of attack can be related to copying or exposing of information, and damaging or altering of the data. Both the security experts we interviewed agreed that copying or exposing of information is a very likely method of attack, while one expert was also certain that modification or altering of data using flawed certificates can also be a likely method of attack. We therefore set the most likely ***Methods*** of attack as *Copy, Expose*, and *Damage, Alter.*

6.3.2.3. Vendors

Casey (2007) in Figure 18 defined the archetype of a business partner who seeks inside information for financial advantage over its competitors as 'Vendor', with a *Hostile* ***intent***. In Section 6.3.1.1, we also identified that the recklessness of vendors can be a possible threat to e-government infrastructures. We define the Reckless Vendor as a business partner providing services to Digipoort who can be a threat due to their reckless actions. Their ***Intent*** is *Non-Hostile*. Lack of attention to password security, making a poor choice of passwords, revealing passwords to others, or scribbling passwords down are some reckless behaviors that can lead to sensitive information disclosure (Bottom, 2000). Below we discuss the attributes, *Trust Level, Methods, and Objectives* of the two types of Vendor threat agents, Vendor Hostile and Vendor Reckless.

TAL attributes

We have summarized all the attributes of Vendor Hostile and Vendor Reckless threat agents in the tailored TAL in Figure 23.

- *Vendor Hostile*
  The attributes of a hostile Vendor were already defined by Casey (2007) in Figure 18. We will not be discussing more about its attributes here, but instead reuse Casey's definition in our tailored TAL. There's however one change related to the *Resources* attribute which we discuss later in this section.

- *Vendor Reckless*
  A vendor is an actor who has internal access to the Digipoort system. From the use case diagram (Figure 10) about re-injecting a message and the vendor functions in Digipoort OTP, it is clear that the interactions of the vendor with the Digipoort information system are much bigger than that of any other actor defined. The ***Access*** attribute is therefore *Internal*.

  The hostile vendor already defined in TAL (Figure 18), intentionally attacks expecting to gain business or technical advantage from that (Casey, 2007). The non-hostile vendor on the other hand, with their reckless actions can cause damage to the system and reputation damage to Logius. Though unintentional, the ***Outcome*** of their actions can lead to *Damage* and *Embarrassment* to the service accepting organization, similar to other *non-hostile* threat agents (Casey, 2007). Like all the other *non-hostile* agents defined in the TAL, the ***Objective*** attribute can be considered as *All of the above/Don't care,* because there is no rational plan executed by the vendor in case of reckless behavior.

  Designing vendor contracts is a very complex process (Brown, Potoski, & Van Slyke, 2006). The vendor contracts contain Service Level Agreements (SLAs) which include the description of services to be provided to the customer, the expected service levels, metrics by which the service levels are measured, the responsibilities of each party, and/or penalties for breach (Lacity & Hirschheim, 1993). The obligation to meet the service levels in the SLAs makes their ***Limits*** attribute as *Legal*.

  Casey (2007) set the *Resources* of a Vendor as that of a formally organized group with a leader (*Team*). The *Vendors* are usually highly technically skilled service organizations. The availability of highly skilled technology and service is one of the reasons why governments outsource the development and maintenance of e-government infrastructures (Yang et al., 2008). A *Vendor* threat agent can therefore be larger and better resourced than a team. For instance, the Digipoort OTP is a service provided by a large IT vendor to Logius. We therefore set the ***Resources*** attribute therefore as *Organization* (also for *Vendor Hostile*). The skill level of a threat agent with resource level as *Organization* is *Adept*, according to (Casey, 2007). The familiarity of the system, the internal access, and the administrative privileges of the vendors providing the service make the vendors highly skilled. The ***Skills*** attribute is therefore set as *Adept.*

  When faced with a cyber-attack, many organizations tend to hush it down. Acknowledging that one's network has been breached can be bad for one's business. It could destroy trust among customers, suppliers, regulators and shareholders (Lucas, 2015). Telang & Wattal (2005), based on an empirical investigation about the effect of vulnerability disclosure on the market value of

companies, mentions that, "the software vendors on an average lose about 0.76% market value when a vulnerability is disclosed". This could be an incentive for vendors to be clandestine about an attack. The ***Visibility*** attribute can therefore be set as *Clandestine*. The ***Motivation*** of the *Reckless Vendor* is *Accidental*, as defined by Casey (2015) for non-hostile actors.

Methods & Objectives

We discuss the *Methods* and *Objectives* of the two vendor threat agent archetypes here. The *Methods* and *Objectives* of Vendor Hostile and Vendor Reckless threat agents have been summarized in the tailored MOL shown in Figure 24.

- *Vendor Hostile*

  The main motivation of the *Vendor* is *Organizational Gain*, as discussed earlier. Vendors have internal access to the infrastructure and manage many critical activities related to the system. The use case model in Figure 10 shows the various activities performed by the vendor for Digipoort OTP. Considering the criticality of the activities performed, the level of trust placed on the vendor is very high. The vendor also performs many of the administration activities of Digipoort OTP, including monitoring and servicing. This gives them a very high trust level within the target organization. The trust placed on a vendor in such instances can therefore be very high. We can consider the ***Trust Level*** to be similar to that of an *Employee* or an *Administrator* of the target organization.

  The incidents list in the Appendix II showed two instances where the vendors acted in a way that was malicious to the target organization. In one incident the vendor was involved in an end of contract dispute over the ownership of assets containing data. In another, the vendor performed an unauthorized downloading of personal information from the target system. The incidents show that the ***Objectives*** of a malicious vendor could be *Theft/Exposure* and *Data Loss*. The likely ***Methods*** of attack by a *Vendor* to achieve their objectives include *Copying* or *Exposing, Denying,* or *Withholding,* and *Taking,* or *Removing.* The *Methods and Objectives* of a *Vendor* have been summarized in the tailored MOL shown in Figure 24.

- *Vendor Reckless*

  The ***Trust level*** is considered to be that of an *Employee* or an *Administrator* of the target organization as discussed above. While discussing the attributes of reckless vendors earlier, we realized that their motivations are accidental and their ***Objectives*** do not have a malicious intent. Their non-malicious objectives can however have negative effects on the infrastructure and the organization. From the incident list in the Appendix II, several incidents were identified that could have happened as a result of the recklessness of the concerned vendor. When asked about the likely effects on the e-government infrastructure as a result of recklessness of a vendor, the security experts we interviewed mentioned *Theft/Exposure, Data loss, and Operations impact.* We also asked about the likely methods of attack of reckless vendors to the experts. They mentioned that copying or exposing of information were very likely methods of attack. They also mentioned that the reckless actions of vendors can lead to destroying,

deleting of data and unavailability of the system. We therefore set the most likely ***Methods*** of attack as *Copy, Expose* and *Destroy, Delete, Render Unavailable*.

6.3.2.4. Civil Activist

A *Civil Activist* is a highly motivated but non-violent supporter of a cause (Casey, 2007). We explain the attributes, *Trust Level, Methods and Objectives* of a *Civil Activist* below.

TAL Attributes

All the attributes corresponding to the Civil Activist threat agent, except the *Motivation* attribute were defined by Casey (2007) as shown in Figure 18. The ***Motivation*** attribute was defined by Casey recently in (Casey, 2015). The civil activist acts for ideological reasons, is motivated by their own sense of morality, justice or political loyalty and is not usually motivated by the desire for profit (Casey, 2015). Their *Motivation* is therefore *Ideology.* We will adopt Casey's definition of the attributes for our tailored TAL. We have summarized all the attributes of a *Civil Activist* in the tailored TAL in Figure 23.

Methods & Objectives

The *Methods* and *Objectives* of a *Civil Activist* have been summarized in the tailored MOL shown in Figure 24. The Civil Activists due to their external access and malicious intent (refer to Figure 23 for the attributes) do not enjoy any sort of trust relation with the system owner or the affected organization. The ***Trust Level*** is therefore *None*.

A look at the incidents in the incident list (Appendix II) related to *Civil Activists* show that all the attacks were undertaken with the goal of 'changing the public opinion or a corporate policy'. Most of the incidents were motivated by their displeasure over certain policies, actions, or regulations by authorities. The likely ***Objectives*** of the civil activists include *Theft/Exposure, Sabotage, Operations Impact, and Embarrassment*. The agents sabotaged websites by posting videos and posting unauthorized messages on it. They accessed databases, servers, and networks in order to expose data on public domains. Through these actions they tried to affect the operations of, and cause embarrassment to the victim organizations. The likely ***Methods*** of attack associated with these objectives include, *Copying or Exposing, Denying or Withholding and Ransom, Destroying or Deleting or Rendering Unavailable, and Damaging or Altering*.

6.3.2.5. Foreign Government Spy

In the incident list in Appendix II, we noticed multiple incidents of foreign governments spying on governmental data and therefore added it to the list of threat agents from past incidents in Table 15. The agent label *Government Spy,* from the TAL (Figure 18) is very similar to the threat agent responsible for these incidents. This actor with attributes similar to that of a *Government Spy*, is labeled as a *Foreign Government Spy*, and is added to the tailored TAL in Figure 23. We explain the attributes, *Trust Level, Methods and Objectives* of a *Foreign Government Spy* below.

TAL Attributes

The *Foreign Government Spy* is a slightly modified version of the *Government Spy* actor defined by Casey (2007). A *Government Spy* is a state-sponsored spy as a trusted insider supporting idealistic goals (Casey, 2007). We defined the *Foreign Government Spy* as a foreign state backed actor who spy on the confidential data of other governments or government agencies. The malicious *Foreign Government Spy* only has external access, unlike the *Government Spy*. The ***Access*** attribute is therefore *External*.

A *Government Spy* acts for ideological reasons (Casey, 2015). A *Foreign Government Spy* could be motivated by their political loyalty to access sensitive information by compromising email systems, databases, networks etc of target government organizations. Political loyalty is classified under the *Ideology* motivation by Casey (2015). The ***Motivation*** attribute of a *Foreign Government Spy* is therefore *Ideology*. All the other attributes of a *Foreign Government Spy* are adopted from Casey's definition of the *Government Spy* threat agent in Figure 18 and is summarized in the tailored TAL in Figure 23.

Methods & Objectives

The *Methods and Objectives* of a *Foreign Government Spy* have been summarized in the tailored MOL shown in Figure 24. A *Foreign Government Spy* does not enjoy any sort of trust relation with the system owner or the affected organization due to their external access and hostile intent (refer to Figure 23 for the attributes). The ***Trust Level*** is therefore *None*.

From the incidents in Appendix II, the involvement of foreign governmental actors in the attacks on government agencies is clear. Their main objective is the theft of sensitive information from the target organizations. The ***Objective*** is therefore *Theft/Exposure*. The method used to achieve this objective mainly included copying the information by intruding into the digital systems of the victim organizations. Therefore we consider the most likely ***Method*** of attack as *Copy/Expose*.

6.3.2.6. Mobster

A *Mobster* is the manager of an organized crime organization with significant resources (Casey, 2007). We explain the attributes, *Trust Level, Methods and Objectives* of a *Mobster* below.

TAL Attributes

All the attributes corresponding to the *Mobster* threat agent, except the *Motivation* attribute were already defined by Casey (2007) as shown in Figure 18. The defining motivation of the *Mobster* agent is *Organizational Gain,* according to Casey (2015). An incident (in Appendix II) involving the *Mobster* threat agent featured the use of a ransomware to restrict access to the system of the target organization. The access to the system was restored once the ransom was payed by the victim. In this case, the motivation is also *Personal Financial Gain.* The ***Motivation*** can therefore be *Organizational Gain & Personal Financial Gain* as shown in Table 12. We will adopt Casey's definition of the attributes for our tailored TAL. We have summarized all the attributes of a Mobster in the tailored TAL in Figure 23.

Methods & Objectives

The *Methods* and *Objectives* of a *Mobster* have been summarized in the tailored MOL shown in Figure 24. Organized cybercrime is increasing as traditional organized criminal groups are gradually moving to more rewarding and less risky operations in cyberspace from their traditional criminal activities. The

groups could involve networks of tens to several thousands of members. Some criminal groups will even have enough resources to create and maintain value chains for the cyber offence on their own. The cybercriminals could employ C2C (criminal-to-criminal) models which make use of crime tools available through the digital networks. They use viruses, Trojans, keyloggers etc to attain the flexibility of controlling, stealing and trading data (Tropina, 2015). Like the other hostile actors, *Mobsters* do not enjoy any trust with the target organization. The ***Trust Level*** is *None*.

The ***Objectives*** of the Mobster agent could be *Theft/Exposure, Data Loss, Sabotage, Operations Impact*, *and Embarrassment*. The security experts we interviewed mentioned that there can be numerous objectives for a *Mobster*. One expert mentioned that all the objectives mentioned above were usually seen with respect to a *Mobster*. When asked about the likely methods of attack by a *Mobster* agent, the experts mentioned that all the methods excluding taking, or removing assets were usually seen as methods of attack associated with a *Mobster*. The ***Methods*** of attack therefore include *Copy, Expose and Deny, Withhold, Ransom and Destroy, Delete, Render Unavailable and Damage, Alter*.

6.3.2.7. Disgruntled Employee

Disgruntled Employees is a threat agent group that involves current or former employees with an intent to harm the organization (Casey, 2007). We explain the attributes, *Trust Level, Methods and Objectives* of a Disgruntled Employee below.

TAL Attributes

All the attributes corresponding to the disgruntled employee threat agent, except the *Motivation* attribute were already defined by Casey (2007) as shown in Figure 18. Even though emotional personal gain can be considered as the motivation of disgruntled employees, Casey (2015) defined the ***Motivation*** more specifically as *Disgruntlement* as shown in Table 12. We will adopt Casey's definition of the attributes for our tailored TAL. We have summarized all the attributes of a *Disgruntled Employee* in the tailored TAL in Figure 23.

Methods & Objectives

The *Methods* and *Objectives* of a *Disgruntled Employee* have been summarized in the tailored MOL shown in Figure 24. Employees have internal access and a higher trust level in the target organizations. Therefore the ***Trust Level*** of disgruntled employees can be as high as *Employee* or even *Administrator* level.

The sample MOL (Figure 20) created by Rosenquist (2009) shows the objectives and methods of a disgruntled employee. The likely ***Objective*** of a disgruntled employee would be to *Sabotage* or cause *Embarrassment* to the organization as seen from the incidents in Appendix II. In the incident relating to the disgruntled employee in Appendix II, the disgruntled employee resorts to copying or exposing of information, and taking or removing valuable assets (including information) from the organization. The most likely ***Methods*** used by a Disgruntled Employee as mentioned by Rosenquist (2009) in Figure 20 includes *Copy, Expose; Deny, Withhold, Ransom; Destroy, Delete, Render Unavailable; Damage, Alter; and Take, Remove.* We therefore adopt these methods as likely to be executed by a *Disgruntled Employee* in our tailored MOL.

6.3.2.8. Internal Spy

The threat agent *Internal Spy* is defined as a trusted insider who gathers data with a simple profit motive. They lead to the theft of IP, PII, or business data (Casey, 2007). We explain the attributes, *Trust Level, Methods and Objectives* of an *Internal Spy* below.

TAL Attributes

All the attributes corresponding to the *Internal Spy* threat agent, except the *Motivation* attribute were already defined by Casey (2007) as shown in Figure 18. The incident list in Appendix II shows an incident where an agent collects and sells confidential information to a tax fraud ring for a profit motive. The ***Motivation*** of an *Internal Spy* can be considered as *Personal Financial Gain,* as shown in Table 12. We will adopt Casey's definition of the attributes for our tailored TAL. We have summarized all the attributes of an internal spy in the tailored TAL in Figure 23.

Methods & Objectives

The *Methods* and *Objectives* of an *Internal Spy* have been summarized in the tailored MOL shown in Figure 24. Internal spies exercise internal access to the assets and can be employees or administrators in the organization (refer to Figure 23 for the attributes). The ***Trust Level*** enjoyed by these agents can be as high as *Employee* or even *Administrator* level.

The ***Objective*** of the *Internal Spy* is to steal valuable data as seen from past incidents in Appendix II, and therefore can be considered under *Theft/Exposure*. The likely ***Methods*** of attacks that these agents use to achieve their objectives as seen from the incidents include copying, or exposing of valuable information assets. The *Methods* therefore include *Copy, or Expose*.

6.3.2.9. Thief

The threat agent *Thief* is defined by Casey (2007) as an opportunistic individual with a simple profit motive. We explain the attributes, *Trust Level, Methods and Objectives* of a *Thief* below.

TAL Attributes

All the attributes corresponding to the *Thief* threat agent, except the *Motivation* attribute were already defined by Casey (2007) as shown in Figure 18. The ***Motivation*** of a Thief can be considered as *Personal Financial Gain,* as shown in Table 12. The incident list in Appendix II shows that a Thief can have internal or external access. An instance where an employee stole an external hard drive was seen among the past incidents, at the same time an office burglary attack was also found. Therefore we consider the ***Access*** attribute as both *Internal* and *External*. We will adopt Casey's definition of the attributes for our tailored TAL. We have summarized all the attributes of a *Thief* in the tailored TAL in Figure 23.

Methods & Objectives

The *Methods and Objectives* of a *Thief* have been summarized in the tailored MOL shown in Figure 24. The common tactics used by the agent, as shown in Table 15, includes theft of hardware goods, or IP, PII or business data (Casey, 2007). The incidents in the Appendix II also show the same trend. As explained

above, a thief can have internal or external access. The ***Trust Level*** can therefore lie in the range of *no trust* for a burglar and *partial* to *administrator* level trust for an employee acting as a thief.

The motivation of a thief is *Personal Financial Gain* as mentioned earlier. From the incidents it is also clear that most of the attacks were driven by a profit motive. The objective of the threat agents during the attacks was to perform theft. The ***Objective*** can therefore be considered as *Theft/Exposure.* The incidents show that the most likely methods of attack include copying, or exposing information, and taking, or removing valuable hardware from the target organizations. For instance stealing an external hard drive was one of the actions taken by a *Thief,* among the incidents seen. In most cases, the theft also led to the exposure of confidential information contained within the hardware. The likely ***Methods*** of attack therefore include *Copy, or Expose* and *Take or Remove*.

6.3.2.10. Reckless Employee

A *Reckless Employee* is a non-malicious current employee who circumvents safeguards for expediency (Casey, 2007). We explain the attributes, *Trust Level, Methods and Objectives* of a *Reckless Employee* below.

TAL Attributes

All the attributes corresponding to a *Reckless Employee*, except the *Motivation* attribute were already defined by Casey (2007) as shown in Figure 18. The ***Motivation*** of a *Reckless Employee* is considered as *Accidental* as shown in Table 12. We will adopt Casey's definition of the attributes for our tailored TAL. We have summarized all the attributes of a *Reckless Employee* in the tailored TAL in Figure 23.

Methods & Objectives

The *Methods and Objectives* of a *Reckless Employee* have been summarized in the tailored MOL shown in Figure 24. Being an employee with internal access the ***Trust level*** enjoyed by these agents can be as high as *Employee* or even *Administrator* level. Incidents in Appendix II related to instances of reckless behaviour by employees of organizations show that it led to the compromise of sensitive information. There were however no malicious intentions and the motivation is *Accidental,* as discussed earlier. The ***Objectives*** of *Reckless Employees* are also non-malicious. Their actions can however lead to data loss, impact on operations and exposure of information assets as seen from multiple incidents in the Appendix II. The likely ***Methods*** of attack that lead to the fulfillment of these objectives include *Copying,* or *Exposing, Destroying,* or *Deleting,* and *Damaging,* or *Altering*. Moreover, the sample MOL developed by Rosenquist (2009) in Figure 20, also show similar methods of attack by a reckless employee.

6.3.2.11. Employee Error

The threat agent *Employee Error* includes current employees who are non-malicious, but unknowingly misuses the system or its safeguards. This could be due to poor processes, unforeseen mistakes, or simple mistakes (Casey, 2007). This agent label is synonymous to the *Employee Untrained* label in the TAL in Figure 18. From the incidents list in Appendix II, it is seen that many of the employee related incidents are due to the errors committed by the employees. The attributes of the *Employee Untrained*

threat agent fits well with the threat agent concerned with these incidents. Therefore, moving forward we mention this threat agent as *Employee Error* to fit the context of incidents.

TAL Attributes

All the attributes of the *Employee Error* threat agent are adopted from attributes of the *Employee Untrained* threat agent defined by Casey (2007) as shown in Figure 18. The ***Motivation*** for an employee committing error is considered as *Accidental* as shown in Table 12. We have summarized the attributes of a *Reckless Employee* in the tailored TAL in Figure 23.

Methods & Objectives

The *Methods and Objectives* of an *Employee Error* threat agent have been summarized in the tailored MOL shown in Figure 24. The ***Trust level*** enjoyed by these agents can be as high as *Employee* or even *Administrator* level. Even though the ***Objective*** of this threat agent is not intentional, their actions can lead to data loss, impact on operations and exposure of information assets as seen from the incidents in Appendix II. The past incidents also show that the likely ***Methods*** of attack include *Copying, or Exposing, Destroying, or Deleting, and Damaging, or Altering*. This is also clear from the sample MOL developed by Rosenquist (2009) in Figure 20.

6.3.3. Tailored TAL & MOL

In the sections 6.3.1 and 6.3.2 we discussed the various threat agents relevant for e-government infrastructure for businesses, and their attributes, methods and objectives. In Figure 23 we summarized the attributes of the threat agents as the **tailored TAL** for e-government infrastructure for businesses.

Threat Agent Attributes		Non-hostile					Hostile							
		End-user (Reckless)	CSP	Vendor (Reckless)	Reckless Employee	Employee Error	Fraudster (End user fraud)	Civil Activist	Foreign Govt Spy	Mobster	Disgruntled Employee	Internal Spy	Thief	Vendor (Hostile)
Access	Internal			x	x	x					x	x	x	x
	External	x	x				x	x	x	x			x	
Outcome	Acquisition/Theft						x			x		x	x	
	Business Advantage								x					x
	Damage	x	x	x	x	x					x			
	Embarassment	x	x	x	x	x		x			x			
	Tech Advantage								x			x		x
Limits	Code of Conduct		x			x								
	Legal	x		x	x		x							x
	Extra-Legal, minor							x				x	x	
	Extra-Legal, major								x	x	x			
Resources	Individual				x	x					x		x	
	Club													
	Contest													
	Team													
	Organization	x	x	x			x	x		x		x		x
	Government								x					
Skills	None												x	
	Minimal					x								
	Operational										x			
	Adept	x	x	x	x		x	x	x	x		x		x
Objective	Copy							x	x			x		x
	Deny													
	Destroy										x			
	Damage										x			
	Take						x			x			x	
	All of the above/Don't care	x	x	x	x	x								
Visibility	Overt					x								
	Covert	x			x		x			x				
	Clandestine		x	x				x	x			x	x	x
	Multiple/Don't care										x			
Motivation	Accidental	x	x	x	x	x								
	Coercion													
	Disgruntlement										x			
	Dominance													
	Ideology							x	x					
	Notoriety													
	Organizational Gain						x			x				x
	Personal Financial Gain						x			x		x	x	
	Personal Satisfaction													
	Unpredictable													

Figure 23: Tailored Threat Agent Library (TAL) for e-government domain

In Figure 24 we summarized the *Trust Level, Methods and Objectives* of the threat agents as the **tailored MOL** for e-government infrastructure for businesses. The tailored TAL and MOL can be used to perform TARA methodology on e-government infrastructure for businesses.

Agent Name	Attacker					Motivation	Objectives	Methods					Limits			
	Access	Trust														
		None	Partial	Employee	Administrator			Copy, Expose	Deny, Withold, Ransom	Destroy, Delete, Render Unavailable	Damage, Alter	Take, Remove	Code of conduct	Legal	Extra-legal, minor	Extra-legal, major
End User (Reckless)	External		x			Accidental	No malicious intent	x		x						
CSP	External		x			Accidental	No malicious intent	x			x		x			
Vendor (Reckless)	Internal			x	x	Accidental	No malicious intent	x		x				x		
Reckless Employee	Internal		x	x	x	Accidental	No malicious intent	x		x	x			x		
Employee error	Internal		x	x	x	Accidental	No malicious intent	x		x	x		x			
Fraudster (End user fraud)	External		x			Organizational Gain and/or Personal Financial Gain	Theft/Exposure	x						x		
Civil Activist	External	x				Ideology	Theft/Exposure, Sabotage, Operations impact, Embarrassment	x	x	x	x				x	
Foreign Govt Spy	External	x				Ideology	Theft/Exposure	x								x
Mobster	External	x				Organizational gain and/or Personal Financial Gain	Theft/Exposure, Data Loss, Sabotage, Operations Impact and Embarrassment	x	x	x	x					x
Disgruntled Employee	Internal		x	x	x	Disgruntlement	Sabotage, Embarrassment	x	x	x	x	x				x
Internal Spy	Internal		x	x	x	Personal Financial Gain	Theft/Exposure	x							x	
Thief	Internal/External	x	x	x	x	Personal Financial Gain	Theft/Exposure	x				x			x	
Vendor (Hostile)	Internal		x	x	x	Organizational Gain	Theft/Exposure, Data Loss	x	x			x		x		

Figure 24: Tailored Methods & Objectives Library (MOL) for e-government domain

6.4. Summary

We answered the third sub-question, "*How can a threat assessment methodology be applied for e-government infrastructure for businesses?*" in this chapter. The main motivation behind this chapter was to tailor the TARA methodology for e-government infrastructure for businesses. In Section 5.4 of Chapter 5 we identified the limitations regarding TAL and MOL for using the TARA methodology for e-government infrastructure for businesses. In this chapter we realized that we needed to tailor the TAL and MOL libraries for e-government infrastructure for businesses.

In order to tailor the TAL and MOL we first identified the threat agents that are relevant for e-government infrastructure for businesses from the use cases of Digipoort OTP and incidents in the public sector we extracted from the publicly available incident database of Privacy Rights Clearinghouse. From the use cases of Digipoort OTP we added End User Reckless, Fraudsters, CSPs, and Vendor Reckless as relevant threat agents for the tailored TAL. From the past incident database we identified threat agents like Employee Reckless, Employee Error, Civil Activist, Foreign Government Spy, Mobster, Employee Disgruntled, Internal Spy, Thief, and Vendor Hostile to be very relevant for e-government infrastructures. We then used the knowledge from Information Security literatures and expert advice to determine the attributes, methods, and objectives of these threat agents. We summarized the results of our analysis in the form of a tailored TAL and MOL in Figure 23 and Figure 24 respectively.

This chapter described the *BIE* phase of the research. By tailoring the TAL and MOL for e-government infrastructure for businesses, we have answered the sub-question 3 that we had put forward in the beginning of this chapter. In the following chapter we will apply the tailored TAL and MOL artifacts to the case of Digipoort PI we discussed in Chapter 4.

APPLICATION

7. Application – Tailored TAL & MOL

This chapter is part of the *Reflection and Learning* phase of the ADR model. In this chapter we perform a minimal version of TARA. More specifically, we apply TARA on a critical asset of Digipoort PI. Digipoort PI is an e-government infrastructure managed by Logius and used for sending messages between businesses and Dutch government agencies. We discussed Digipoort and its two types – Digipoort OTP and Digipoort PI in Chapter 4. In this chapter we apply the tailored TAL, and MOL we developed in the previous chapter by applying the TARA methodology to one critical asset of Digipoort PI. The critical asset we selected for this analysis is the PKI (also called the *Key Management System* in general) of Digipoort PI. Thereby we answer the fourth sub-question.

SQ 4: *What are the results of applying the tailored threat agent centric threat assessment methodology in a practical case study?*

In Section 7.1 we discuss the TARA methodology applied on Digipoort PI, and in Section 7.2 we describe the sources we used to collect knowledge for the analysis. Further in Section 7.3 we explain the results of the application of methodology. Subsequently in Section 7.4 we discuss the insights we obtained from the application of the methodology, followed by a summary of the chapter in Section 7.5.

7.1. Methodology

The TARA methodology we use is different from the Intel TARA methodology shown in Figure 21 because,

- We use the tailored TAL and MOL artifacts for e-government infrastructure for businesses we developed in Chapter 6 to understand the threat agents, their methods and objectives.
- We identify the critical assets that are associated with the threat agents early in the methodology, in order to focus our analysis on one critical asset.
- We mentioned in Chapter 5 the unavailability of the Common Exposure Library (CEL) - an artifact which enumerates known information security vulnerabilities and exposures at Intel associated with the TARA, for our research due to its confidential nature. We overcome this absence by creating sample attack scenarios on the asset under focus from each threat agent.

As shown in Figure 21, the starting point of TARA methodology is the full list of threat agents, and their methods and objectives, which we already created in the form of the tailored TAL and MOL. The following steps (shown in Figure 25) show how we apply the TARA methodology on the critical asset.

Step 1: Filter and Prioritize Threat Agents, Methods and Objectives.

In the TARA process explained by Rosenquist (2009), this step involves prioritizing the highest risk threat agents and identifying their likely methods and objectives. Intel uses a baseline risk level created by senior security experts through regular review and ranking of current threat levels to prioritize the threat agents. Further they identify the likely methods and objectives of threat agents using the MOL. Since we are applying the TARA methodology for the first time to an e-government infrastructure, we do not yet have a baseline risk level for prioritizing the threat agents. Therefore we prioritize the threat

agents relevant for Digipoort PI using a *relevance score*. Then we identify the likely methods and objectives for the threat agents depending on the critical asset we choose for the analysis. This is achieved in the following way.

a) *Prioritize threat agents and understand critical assets*

In order to identify the threat agents and critical assets that are most relevant to Digipoort PI, we use the tailored TAL (Figure 23) to prepare a questionnaire based on the characteristics of the threat agents. We use the questionnaire to interview experts in the implementation and working of Digipoort PI at Logius. Based on the inputs from the interview the critical asset for analysis is determined. In order to prioritize the threat agents we introduce a relevance score for each threat agent. The relevance score is an ordinal representation of the relevance of the threat agents with respect to Digipoort PI. The expert is explicitly asked to rate the threat agents on a scale from 1 to 5, depending on the relevance of the threat agents for Digipoort PI. The ordinal scale measures the relevance in an increasing order, with 1 being the least relevant and 5 being the most relevant. While prioritizing the threat agents, we will choose the threat agents with top three relevance scores for our further analysis. The interview protocol is explained in Section 7.2.

b) *Identify the likely methods and objectives of Threat Agents*

Here we select the likely methods and objectives of the threat agents from the tailored MOL (Figure 24). All the methods of attack from the tailored MOL for a particular threat agent might not be applicable to the critical asset under analysis. We therefore concentrate on the likely methods of attack that are selected based on the critical asset selected for the analysis.

The output of this step is the prioritized list of threat agents, their objectives, motivations and likely attack methods.

Step 2: Identifying Vulnerabilities and Exposures.

In the original TARA process explained by Rosenquist (2009), Intel uses the CEL library to enumerate the vulnerabilities of the assets. For our research, we do not have a CEL and therefore no list of vulnerabilities to choose from. We therefore proceed in the following way.

a) *Develop likely attack scenarios*

We develop likely attack scenarios for each threat agent based on the likely methods of attack we identified in the previous step. Background knowledge on the Digipoort PI infrastructure will be used to create the attack scenarios for each relevant threat agent. We will make use of technical artifacts available at Logius, and past incidents related to the particular threat agents to create the attack scenarios. We also interview experts in Digipoort PI at Logius to understand the likeliness of the attack scenarios. The interview protocol is explained in Section 7.2.

b) *Identify minimum controls necessary*

We look at the minimum security controls necessary for the assets to mitigate the threat scenarios we created earlier. We obtain knowledge about minimum controls from documents on Information Security Standards like the ISO 27001/27002, Baseline Informatiebeveiliging Rijksdienst (BIR) – a standard for

security information management in the government agencies, ISO 9001, and also from literature on the critical asset under focus.

c) *Identify the existing controls on the asset and exposures*

Here we look at the existing controls necessary for the assets to mitigate the attacks by threat agents. We consult internal documents related to the technical implementation of Digipoort PI, the book – 'Challenging the Chain' by Bharosa et al. (2015), information security documents and also interviews of the experts in Digipoort PI at Logius to understand the existing controls. The interview protocol is explained in Section 7.2. We compare the minimum controls which we identified earlier with the existing controls to identify the exposures. Insufficient controls against a particular threat agent attack method cause exposure for the asset.

Based on the information gathered in this step, we develop conclusions about the threat agents as a risk to the critical asset under analysis.

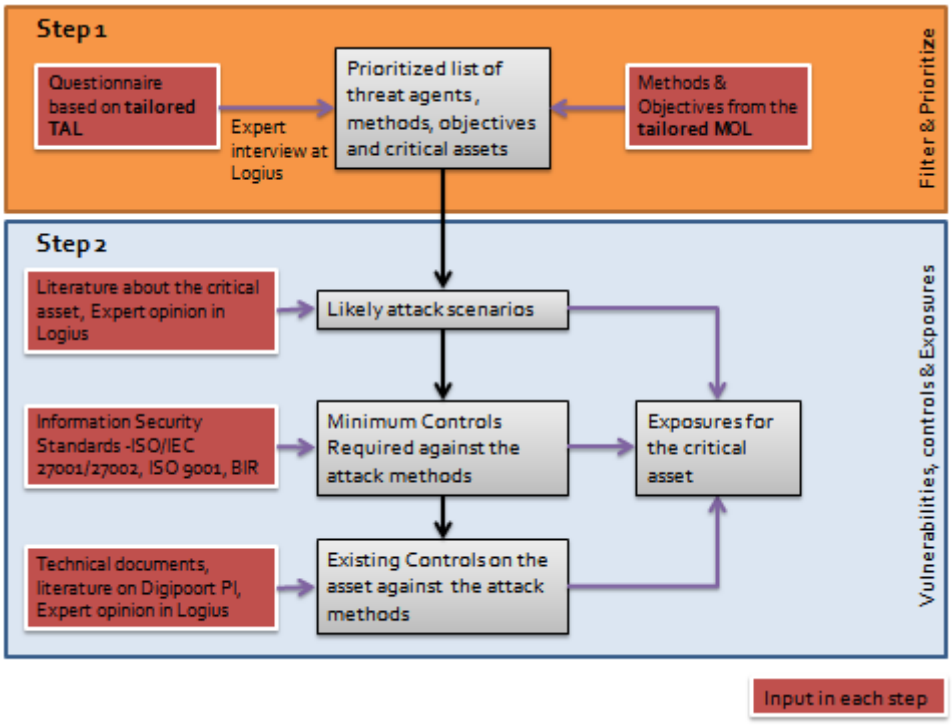

Figure 25: Tailored TARA methodology for Digipoort PI

By executing the steps mentioned above, the TARA methodology can be used to understand the threat landscape of the critical asset. In the following section we discuss the results of applying the TARA methodology on one critical asset of Digipoort PI. In Appendix V we have also shown a broader application of the TARA methodology on Digipoort PI.

7.2. Implementation - Resources

In this section we describe the resources that we used to gather knowledge at the various stages of application of the TARA methodology.

Interview Protocols

We conducted two sets of interviews for collecting knowledge during the various steps in the application of the TARA methodology (The identities of interviewees are not revealed to protect confidentiality).

- *Interview Set 1 – Prioritizing threat agents using TAL*
  We interviewed Logius_Expert1, an expert in Digipoort PI using a TAL based questionnaire to prioritize the threat agents and identify the critical assets of Digipoort PI. For instance, in order to understand the relevance of *Internal Spy* as a threat agent on Digipoort PI we ask the following question.

  "*How easily can the information flowing through Digipoort PI be used by an actor with internal access for financial gain? How relevant are internal spies as a threat agent for Digipoort PI on a scale from 1 to 5?"*

  And to understand the critical assets associated with an Internal Spy, we ask the following question.

  "What assets can be compromised by a threat agent through internal access? What would be the impact?"

  We then analyze the responses of the expert for each threat agent and create a list of threat agents and their relevance scores. The threat agents are then prioritized based on their relevance scores. The questionnaire and the responses of the expert are shown in Appendix IV.

- *Interview Set 2 – PKI of Digipoort PI*
  We interviewed the following experts to gather knowledge about the PKI asset (the critical asset we chose for analysis) of Digipoort PI, its controls and exposures.
  - Logius_Expert2, PKIOverheid
  - Logius_Expert3, Certificate Manager, Digipoort
  - Logius_Expert4, Incident Manager, Digipoort
  - Logius_Expert5, Interim Ketenbeheerder, VENDOR1

  The questions were specifically aimed at understanding the specific characteristics of the PKI of Digipoort PI, its implementation, accesses, security controls, and the likelihood of certain attack scenarios. The questionnaire and the responses of the experts are shown in Appendix IV. A summary of responses was created as shown in Table 26, which was then used in analyzing the threat landscape of the PKI of Digipoort PI.

Technical Artifacts

We referred to documents obtained from Logius to understand the technical aspects of the Key Management asset and to identify the existing controls on the asset. For this we used Process Infrastructure documentations of Digipoort PI, the book – 'Challenging the Chain' by Bharosa et al. (2015), and other information security documents.

Standards

We referred to information security standards like ISO 27001/27002, ISO 9001, and the Baseline Informatiebeveiliging Rijksdienst (BIR) to identify the minimum controls required against the various threat agent attack methods. We also referred to the Program of Requirements (PoR) maintained by the PKI Overheid department of Logius in order to understand the controls for CSPs (Logius, 2015n).

7.3. Results

In this section we discuss the results of applying the TARA methodology on the *Key Management* asset of Digipoort PI. First, we discuss the results of Step 1 – the critical asset selected for the analysis, the prioritized list of threat agents, and the likely methods and objectives. Then we discuss the outputs of Step 2 - the sample attack scenarios of the threat agents, the controls and exposures for the asset. Subsequently, we summarize the risk due to the various threat agents on the asset.

Step 1: Filter and Prioritize Threat Agents, Objectives and Methods.

Critical Assets

Based on the first set of interview we conducted with Logius_Expert1 at Logius, we identified the *Key Management System (or the PKI)* as one of the most critical assets for Digipoort PI (as shown in Interview Set 1 - Appendix IV). The *Key Management System* (KMS) manages the private and public key pairs of Digipoort PI. The key pairs are used by Digipoort for establishing a secure TLS connection with end users at the transportation layer and are also used for encrypting the messages at the application layer (Bharosa et al., 2015). The data transfer between the end users and the governments will cease to be secure, if the private key of Digipoort is compromised. This makes the *Key Management System* a critical asset of Digipoort PI. We already discussed the PKI in Section 4.3 of Chapter 4. The subsequent application of the TARA methodology is performed on the *Key Management* asset of Digipoort PI. The expert also mentioned other assets of Digipoort PI and the threat agents which can be directly responsible for attacking them as shown in Table 17. According to the expert, the CSP is the most direct threat agent to the KMS asset. However, in order to make a comprehensive analysis we will consider all the threat agents in the prioritized list of threat agents for Digipoort PI. The prioritized list of threat agents is explained below.

Prioritized List of Threat Agents

The relevance scores of threat agents with respect to Digipoort PI based on the responses from the interview are shown in Table 16.

Table 16: Relevance scores of Threat Agents associated with Digipoort PI

Threat Agent	**Relevance Score** (1 - least relevant to 5 - very relevant)
End User Reckless	4
Fraudster	2
CSP	4
Vendor Reckless - External vendors	5
Vendor Reckless - Internal vendors	2
Vendor (Hostile)	-
Employee Disgruntled - Vendor	4
Employee Disgruntled - Logius	3
Employee Reckless - Logius	3
Employee Error - Logius	3
Civil Activists	1
Foreign Government Spy	1
Mobster	1
Internal Spy	3
Thief (External)	-
Thief (Internal)	1

We prioritized the threat agents for further analysis based on their relevance scores. The threat agents with the top three relevance scores are considered to be very relevant for Digipoort PI and will be analyzed with respect to the *Key Management* asset.

The threat agents like *Vendor (Hostile)* and *Thief (External)* were not rated because the expert found them irrelevant for Digipoort PI. When asked about the intentional actions of a hostile Vendor on Digipoort PI, the expert said "*I don't think that a vendor acting intentionally against Digipoort PI is relevant, although employee disgruntlement at the vendor seems relevant*". Similarly for a Thief the expert said "*I do not know if there have been cases of theft in the past. But, a burglar has no relevance. Internal theft could be relevant but really low*". The threat agents like the *Civil Activists*, the *Foreign Government Spy*, and the *Mobster* were also rated very low because of the difficulty involved in attacking Digipoort PI externally, and because detection is easier due to the use of digital certificates. This can reduce the motivation of these external threat agents to attack Digipoort PI, because we can see from the tailored TAL (Figure 23) that all these agents prefer to be covert or clandestine about their actions. The ease of detection of the users of Digipoort PI is also the reason why Fraudsters were rated low by the expert. While rating the relevance of the Fraudster threat agent, the expert mentioned that "*If you access the system, the system knows exactly who it is using the digital certificate. A fraudster is immediately identified. So the end user is not likely to perform fraud on Digipoort PI*".

We also asked the expert to make a differentiation between the internal and external vendors of Digipoort PI while talking about the relevance of Vendor Recklessness. The expert gave a very high relevance score for external vendors, but a low relevance score for internal vendors. The expert supported this difference in score by saying that the internal vendors do not have any real access to the Digipoort system and that no assets are directly affected by the internal vendors. Vendor Recklessness is

therefore mainly associated with external vendors and not internal vendors. All the relevant threat agents for Digipoort PI, with a short description, the assets that could be directly compromised by these threat agents and their potential impacts are shown in the prioritized list of threat agents in Table 17.

Table 17: Prioritized threat agent list for Digipoort PI (Top 3 relevance scores)

Threat Agent	Description	Critical Assets Compromisable	Impact - General
End User (Reckless)	Users of Digipoort PI (businesses/intermediaries) who can cause unintentional damage to the system, due to their reckless behavior or carelessness.	Process Infrastructure	Low to high business impact due unavailability of the process infrastructure.
CSP	Third party certificate providers for the Public Key Infrastructure (PKI), who provides keys or certificates to the users. Errors made by CSPs can have a big impact on the Digipoort PI system.	Key management system or the PKI	High business impact due to unavailability of the PKI.
Employee Reckless - Logius	A non-malicious current employee of Logius who circumvents safeguards for expediency.	Information assets, Confidentiality of the processes	Increased vulnerability of the system
Employee Error - Logius	A non-malicious current employee of Logius, who follows poor processes, makes unforeseen mistakes, or simple mistakes.	Information assets, Confidentiality of the processes	Increased vulnerability of the system
Disgruntled Employee - Logius	Current or former employees of Logius with intent to harm the organization.	Information assets, Confidentiality of the processes	Increased vulnerability of the system.
Vendor Reckless	External service providers of Digipoort PI with internal access, and acting in a reckless or careless manner. Includes also employee recklessness or error at the vendor.	Software, and hardware assets	1. Partial unavailability and business impact due to software error. 2. Total unavailability and high business impact due to hardware problems.
Disgruntled Employee - Vendor	Current or former employees of Vendors with intent to harm the organization.	Software, and hardware assets	Total unavailability and high business impact due to compromise of the software or the hardware.
Internal Spy	A trusted insider who gathers data with a simple profit motive. They lead to the theft of IP, PII, or business data.	Information assets, Confidentiality of Digipoort PI	Financial losses, Reputation damage

Likely Methods & Objectives

We mapped the threat agents with their methods and objectives from the tailored MOL. Based on the attributes of the threat agents and the characteristics of the *Key Management* asset we explain here why some methods of attack are more likely for the threat agents. The likely methods of attack for each threat agent on the *Key Management System* are highlighted in Table 18. End Users are involved in the transfer of information with Digipoort PI using the certificates they buy from the CSPs. Their reckless behavior in handling the security of their certificates can affect the Digipoort system interacting with them. A compromise of the end user certificate could lead to exposure of key information of Digipoort PI, but cannot cause any destruction or deletion in the *key management* asset. CSPs issue service

certificates for end users and also governmental organizations like Logius. The Diginotar incident already showed that a compromise at the CSP in issuing digital certificates can lead to exposure of the data and altering of the *Key Management System*. Therefore we consider them as likely methods of attack due to CSP recklessness.

Logius is responsible for purchasing the service certificates for Digipoort PI from the CSPs. The Certificate Manager is an employee of the *Keteninformatiediensten* (KD) and is responsible for purchasing the certificates from the CSPs. VENDOR1, the software vendor of Digipoort PI generates two files in their server, a PEM (Privacy Enhanced Mail) file that contains the PKCS#12 standard private key and a CSR (Certificate Signing Request) file which contains the corresponding public key and details about the subscriber of the certificate (Logius in this case). The private key is stored securely in the server while the CSR file is sent to the Certificate Manager at Logius, who files it with the CSP for signing. When the certificate is validated, the Certificate Manager downloads the CSP validated CER (a file extension for a certificate) file. The Certificate Manager then sends it to VENDOR1 via email for installation in the servers. The recklessness and errors made by the Certificate Manager in handling the CSR or CER file could lead to exposure of the contents of the file and revocation of certificates leading to unavailability of the PKI. A disgruntled Certificate Manager could lead to exposure, and alteration or damage to the keys in the *CER* file. The CER file contains the public key of Digipoort PI and the details binding the subscriber of the certificate (Logius in this case) to the public key, signed using the private key of the CSPs.

The *CER* files sent by the Certificate Manager of Digipoort PI are installed by the software vendor – VENDOR1, on the servers of Digipoort. VENDOR1 is therefore responsible for the generation, implementation and maintenance of the key pairs of Digipoort PI. VENDOR2 (infrastructure vendor) hosts the servers on which the certificates are installed. Vendor Recklessness can cause the exposure of the private key and unavailability of the entire asset. A disgruntled employee at the Vendor has a higher relevance than a disgruntled employee at Logius. This is due to the formers internal access to the asset. According to Logius_Expert1, "E*mployee archetypes of the vendor have higher relevance because they have deeper access to the system. Real disgruntled active vendor employees are the highest threat agent because they have internal access*". Since a disgruntled employee does not care about being detected (based on their *Visibility* attribute), they could take almost any method available to destroy or damage the asset. Similarly, an Internal Spy can be more relevant if they are on the vendor side. He also said that, "*The easiness with which an Internal Spy can access valuable information from Digipoort PI would depend on where the threat agent is; at the vendor side it is easier. At the Logius side it is not very easy but not impossible".* It is therefore easier for an internal spy at VENDOR1 or VENDOR2 to expose valuable information like the private key of Digipoort for a profit motive.

Table 18: Prioritized Threat Agents, and their likely Objectives & Methods

Threat Agent	Motivation	Objectives	Methods				
			Copy, Expose	Deny, Withhold, Ransom	Destroy, Delete, Render Unavailable	Damage, Alter	Take, Remove
End User Reckless	Accidental	No malicious intent	x		x		
CSP	Accidental	No malicious intent	x			x	
Employee Reckless - Logius	Accidental	No malicious intent	x		x	x	
Employee Error - Logius	Accidental	No malicious intent	x		x	x	
Employee Disgruntled - Logius	Disgruntlement	Sabotage, Embarrassment	x	x	x	x	x
Vendor Reckless	Accidental	No malicious intent	x		x		
Employee Disgruntled - Vendor	Disgruntlement	Sabotage, Embarrassment	x	x	x	x	x
Internal Spy	Personal Financial Gain	Theft/Exposure	x				

In the following section we discuss the likely attack scenarios, controls and exposures on the *Key Management* asset due to these threat agents.

Step 2: Identifying Vulnerabilities and Exposures for Key Management System

Likely Attack Scenarios

The following attack scenarios were devised for the *Key Management* asset based on the likely methods and objectives of the threat agents we identified earlier.

- *End User Reckless*

  Every end user needs to have a PKIOverheid service certificate to connect to Digipoort PI. This they buy from any of the commercial CSPs in the market (Bharosa et al., 2015). The key pair is generated in the end user system for a PKCS#10 certificate and by the CSP for a PKCS#12 certificate (Logius, 2015a). The private key of the user is then transferred in a secure manner to the end user. In either case, the private key has to be securely stored away from any unauthorized access to it. There's no direct impact on the *Key Management System* of Digipoort due to end user recklessness. However, we mention here a scenario where the Key Management System can be affected by the recklessness of an end user. Fox-IT in its blog explains a similar scenario where certificates were duplicated by factoring their 512 bit RSA keys (Fox IT, 2015).

a) Company A neither has a strong password policy nor an anti-virus installed in their key management server. An ensuing brute force attack led to the compromise of their private key which is now used by the attacker to impersonate Company A in communicating with Digipoort. The attacker now has access to the information flow and the public key of Digipoort PI. He derives the private key of Digipoort PI by a brute force attack on the RSA encryption of Digipoort PI leading to compromise of the Key Management System.

- *CSP*

  One very important function of CSPs in the Netherlands is to issue PKIOverheid service certificates to the end users for connecting to Digipoort PI or other similar e-government services. In this regard the CSPs also issue certificates to Logius for its Digipoort PI system. The following attack scenarios were devised from various incidents associated with CSPs in the past (Barreira et al., 2013).

  a) The private key of a CSP is compromised due to lack of minimum security controls like strong passwords, or an anti-virus on the cryptographic modules of the CSP. All the certificates issued by the CSP and signed with their private key therefore cannot be trusted anymore. The certificates of Digipoort PI were also issued by the same CSP. The certificates and keys of Digipoort PI therefore cannot be trusted anymore and all have to be revoked and replaced leading to considerable business impact.

  b) Digipoort PI signed its certificates with a CSP. The CSP erroneously issues intermediate CA certificates to an entity, but were meant to be user certificates. An attacker uses the intermediate certificate to generate rogue certificates. The rogue certificates could have been used to communicate with Digipoort PI. This causes exposure of the information flow through Digipoort PI. Moreover, this leads to damage to the key management asset of Digipoort PI because the certificates issued by the CSP cannot be trusted anymore leading to revoking of the certificates and considerable business impact.

  c) The Certificate Revocation List (CRL) of the CSPs lets Digipoort PI know which certificates are revoked. In this case the CSP did not include a link to the CRL location for revocation checking in the user certificates. Digipoort PI continues to communicate with a revoked certificate, leading to possible exposure of information flow through Digipoort PI.

  d) The Online Certificate Service Protocol (OCSP) is not maintained properly by the CSP. The OCSP is used by services to access the CRL in real time. Due to this the updated CRL list cannot be accessed in real time by the key management system of Digipoort PI. This leads to wrongful authentication of users with revoked certificates, and possible exposure of information flowing through Digipoort PI.

- *Employees at Logius*

  Employees at Logius do not have any physical or logical access to the keys implemented in the servers of Digipoort PI. However the Certificate Manager at the KD is responsible for purchasing the certificates from the CSPs and also handling the CER files which contain the public key and identification details of Logius. We devised the following threat scenarios associated with the employees of Logius.

  Reckless

  a) The Certificate Manager should authenticate himself using a username and password to log into the portal of the CSP from where he can download the CER files. The CER file contains the public key

information of Digipoort PI signed by the CSP. While in his absence, he gives his credentials to employee X who is not a Certificate Manager to download the CER files on his behalf. Employee X uses the Certificate Manager's credentials to download the CER files. She/he now has unauthorized access to the files which contain information about the public key of Digipoort PI. This could lead to exposure of the public key information.

b) The Certificate Manager should authenticate himself using a username and password to log into the portal of the CSP from where he can download the CER files. The CER file contains the public key information of Digipoort PI signed by the CSP. He downloads a CER file to send it to the supplier (VENDOR1) for installing the certificate in the Digipoort server. The file is sent to the supplier via email. He uses his personal email id for sending the CER file to save time. This could lead to exposure of the public key information.

Error

c) The Certificate Manager should authenticate himself using a username and password to log into the web portal of the CSP from where he can download the CER files. The CER file contains the public key information of Digipoort PI signed by the CSP. He downloads a CER file to send it to the supplier (VENDOR1) for installing the certificate in the Digipoort server. The file is sent to the supplier via email. He unknowingly sends the CER file to a person outside the Logius network.

d) The Certificate Manager receives a CSR from VENDOR1 which is not correct. He applies for the certificate to the CSP without realizing the error in CSR. The CER file is created with the wrong CSR. The CER file is sent by the Certificate Manager to VENDOR1, which is then installed in the Digipoort PI server. However, the Digipoort service fails in production due to the incompatible certificate and the public-private key pair.

Disgruntled

e) The Certificate Manager at Logius is disgruntled due to some personal grudges with the organization. He takes revenge by logging into the portals of CSPs and downloading the CER files of Digipoort certificates. The CER file contains the public key information of Digipoort PI signed by the CSP. He then knowingly sends the CER files outside the Diginetwerk to external parties, causing exposure of the public keys.

f) The Certificate Manager at Logius is disgruntled due to some personal grudges with the organization. He takes revenge by logging into the CSP portals and downloading the CER files of Digipoort certificates. The CER file contains the public key information of Digipoort PI signed by the CSP. She/he alters the CER files before sending it to the supplier (VENDOR1). VENDOR1 install the certificates and PKI of Digipoort PI fails due to the incompetent certificates.

g) The Certificate Manager at Logius is disgruntled due to some personal grudges. He resigns from Logius, but still accesses the CER files from the CSP certificate stores online using his credentials. He misuses the CER files by exposing the CSP signed certificate to external entities.

h) The Certificate Manager at Logius is disgruntled due to some personal grudges. He resigns from Logius, but sends several CER files he downloaded using his credentials to his personal email id before leaving. He plans to expose the information in the CER files to external parties. The public keys along with other details about Logius are exposed.

- *Vendors*

  The following threat scenarios show the ways in which the *Key Management System* can be compromised due to recklessness and disgruntled employees at the vendors. The public and private keys are installed by VENDOR1 in the servers of Digipoort PI. The public key which is used for encryption is available publicly while the private key used for decryption is stored securely in the server. The servers are hosted by VENDOR2 at their data centers.

  Reckless

  a) Mr. X is an administrator at VENDOR1. He wrote down the password to the key server on a piece of paper for convenience. The paper wasn't shredded and ended up in the dumpster. A dumpster diving actor obtains the access credentials to the key server as a result. This could lead to the compromise of the key server and exposure of the private key.

  b) Mr. X is an employee of VENDOR1. A social engineering attacker tricks Mr. X into using a malware affected USB stick on the computer connected to the key server. The malware compromises the server and leads to exposure of the private key of Digipoort PI.

  c) An employee at VENDOR2 accidentally lets an unauthorized person tailgate into the building where the key server is housed. The person accesses the server and manages to steal the private key from the server.

  d) An error in the server led to the generation of an incorrect CSR. The error was overlooked during validation and the CSR was sent to the Certificate Manager at Logius for certificate creation. The Certificate Manager sends the CSR to a CSP who creates an invalid certificate with the CSR. The CER file generated is downloaded by the Certificate Manager from the CSP certificate store and sent to VENDOR1 for installation in the server. VENDOR1 installs the public certificate (CER file) in the server. While in production, the TLS connections with clients fail because of the invalid public certificate. This causes unavailability of the key management system and the Digipoort PI service.

  Disgruntled

  e) A disgruntled administrator at VENDOR1 has access to the server in which the private key of Digipoort PI is stored. He shares his access credential information with an external attacker. External attackers misuse credentials to steal the private key stored in the server (possibly over the network). The key system is compromised and communications are insecure. Logius now has to revoke the certificates. VENDOR1 has to generate new keys and get new digital certificates from the CSP.

  f) A disgruntled administrator at VENDOR1 has access to the server in which the private key of Digipoort PI is stored. He knows the location of the PEM file on which the private key is stored. He copies the private key and shares it with an external attacker. The key system is compromised and communications are insecure. Logius now has to revoke the certificates. VENDOR1 has to generate new keys and get new digital certificates from the CSP.

  g) A disgruntled administrator at VENDOR1 disables the anti-virus application in the key server. The key server is now unprotected and could become vulnerable to external attackers.

  h) A disgruntled non-administrator employee at VENDOR1 breaks into the server in which the private key of Digipoort PI is stored. He finds the copies the private key and shares it with an external attacker. The key

system is compromised and communications are insecure. Logius now has to revoke the certificates. VENDOR1 has to generate new keys and get new digital certificates from the CSP.

i) Former administrator employee at VENDOR1 is disgruntled. He shares his access credentials and details regarding the implementation and location of the keys of Digipoort PI in the server to an external entity. The attacker now clearly knows where to look for in the server to copy, alter or damage the keys of Digipoort PI.

j) A disgruntled employee at VENDOR2 walks into a server room where the key server of Digipoort PI is housed. He physically sabotages the server in which the private key of Digipoort PI is stored. The server could malfunction and become unavailable for performing the encryption or decryption functions for Digipoort PI.

k) Administrator employee at VENDOR2 is disgruntled and shares confidential information like the make and type of server used for storing the private key of Digipoort PI to hostile actors. The hostile actors try to physically access the server in which the key is stored. This can jeopardize the security of the private key of Digipoort PI.

- *Internal Spy*

  An internal spy is a very clandestine actor with a profit motive. The following threat scenarios were devised to demonstrate how an internal spy can expose information regarding the keys of Digipoort PI.

  a) An internal spy at VENDOR2 physically breaks into the server hardware where the private key of Digipoort PI is stored. He then steals the private key of Digipoort PI and sells it to an external attacker.

  b) An internal spy uses Social Engineering techniques (blackmails, bribes, coercion) on the administrators at VENDOR1 to get access to the server of Digipoort PI where the private key is stored. She/he then sells the private key to an external attacker.

  c) An internal spy in Logius compromises Diginetwerk by planting malware on several computers in Logius. This gives the spy agency access to the network communications. The spies are able to monitor the communications of the administrators of the key management system. They compromise the email account of a Certificate Manager of Digipoort PI and steal the CER file sent to VENDOR1. The CER file contains information regarding the public key of Digipoort PI.

  d) An internal spy in VENDOR1 compromises the VENDOR1 network by planting malware on several computers in VENDOR1. This gives the spy agency access to the network communications. The spies are able to monitor the communications of the administrators of the key management system. They spy on the details regarding the location of the private key and the access credentials to the server in which it is stored. The private key is stolen by accessing the servers using the information collected.

Controls and Exposures

A comparison of the minimum controls required and the existing controls for the *Key Management System* asset against the likely attack scenarios we identified earlier for each threat agent is discussed below. The resulting exposures due to these threat agents are thereby identified. The tables 19 to 23

show the minimum controls, existing controls, and possible exposures for the asset due to each threat agent.

- *End User Recklessness*
  The threat scenario we described for the end user involved the loss of private key of a company due to its reckless behavior. A private key loss for the end user communicating with Digipoort PI can lead to the compromise of information being transmitted between Digipoort and the end user. However, any exposure of the private key of Digipoort PI due to this is unlikely. From Table 19 we realize that the existing controls can sufficiently mitigate the attack methods due to a reckless end user. Some controls like the use of CRL guarantee security by design against such compromise of certificates. Moreover, Digipoort PI also uses strong encryption and key algorithms as mandated by the NCSC that makes the brute force attack on the private key nearly impossible. Digipoort PI uses the NCSC mandated 2048 bit RSA keys and SHA – 256 algorithm for hashing (Bharosa et al., 2015; Wijk, 2015). Researchers have in the past cracked the 1024 bit RSA encryption through various techniques (Digicert, 2015; Network World, 2010). However, some researchers mention that breaking a 2048 bit RSA encryption using a standard desktop computing power would take over 6.4 quadrillion years. It would cost an attacker an immense amount of time and resources even with the best computing power available in the world to successfully attempt a brute force attack on the 2048 bit RSA key (Digicert, 2015). We therefore conclude that an attack of similar proportions on the *Key Management* asset of Digipoort PI is highly unlikely and that the exposure due to a reckless end user on the *Key Management* asset of Digipoort PI is very low.

Table 19: End User Reckless - Controls & Exposures for Key Management Asset

Threat Agent	Attack Scenarios	Minimum Controls Required	Existing Controls	Possible Exposures
End User Reckless	a) Company A neither has a strong password policy nor an anti-virus installed in their key management server. An ensuing brute force attack led to the compromise of their private key which is now used by the attacker to impersonate Company A in communicating with Digipoort. The attacker now has access to the information flow and the public key of Digipoort PI. He derives the private key of Digipoort PI by a brute force attack on the RSA encryption of Digipoort PI leading to compromise of the Key Management System.	ISO 27001/27002; BIR; ISO 9001 a) Rules for acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented. b) Users shall only be provided with access to the network and network services that they have been specifically authorized to use. c) Strict rules for authentication and authorization of end users.	Rules for acceptable use a) An interface service specification describes how and under what conditions a connection can be set up between two systems. It contains logistical agreements for the correct addressing, reading, exchanging and processing of messages, as well as agreements for safe and reliable message transmission. It mandates that the certificates should be used by end users in a safe environment. Authentication/Authorization b) A two-way TLS	The 2048 bit RSA keys are nearly impossible to break with contemporary technologies. Exposure to the private key of Digipoort PI due to recklessness in managing own PKI by end users is very low.

Threat Agent	Attack Scenarios	Minimum Controls Required	Existing Controls	Possible Exposures
		d) Strong rules for validation of the certificate. <u>Other</u> e) RSA key has to be of a sufficient length. According to the current standards set by the NCSC the RSA key has to be at least 2048 bits in length and the hash function should be at either SHA – 512, SHA – 384, or SHA – 256.	connection using client and server certificates ensure that reporting and receiving parties are who they claim to be. c) The identity established in the authentication is then used for checking the claimed authorization by checking if there is a valid approval (permission) in a trusted registry. <u>Validation</u> d) During message submission, Digipoort checks the validity of the digital signature. Furthermore, based on the CRL, Digipoort verifies with the CSP that a certificate has not been withdrawn. <u>RSA key security</u> e) The Digipoort PI uses an RSA algorithm with a modulus length of 2048, and an SHA – 256 hash function.	

- *CSP*

  Table 20 shows the controls and exposures for the *Key Management* asset from a CSP threat agent. The CSPs operate according to the strict guidelines in the Program of Requirements (PoR), a standard based on the European standards and the Dutch law (Logius, 2015n). There are strong controls in place to mitigate the attacks on the *Key Management System* and to maintain the trust hierarchy involving the CSPs. Exposures could result therefore from not the lack of controls but the failure to implement these controls properly (Meulen, 2013)

  According to Logius_Expert2 from PKIOverheid (Interview set 2 - Appendix IV), the existing requirements on network security, the baseline requirements for PKI, and the PoR the CSPs are mandated to follow makes the scenarios mentioned in the table unlikely to happen in the case of Digipoort PI. The scenario (a) mentioned in Table 20 is similar to what happened in the case of DigiNotar in 2011. The controls in the PKI infrastructure have been strengthened post Diginotar, especially aiming at consistent incident reporting and stronger auditing of CSPs by external auditors and Logius. The scenario (b) can be a very serious exposure if it happens. Digidentity – commercial and Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG) - government are two out of the seven CSPs who can create intermediate CAs (Logius, 2015b). However the

controls limiting the ability of CSPs to issue intermediate certificates without notifying Logius are in place which makes a wrongful issuance of intermediate certificates unlikely but nonetheless very serious. The scenario (c) is avoided by the PoR mandated use of templates for issuing digital certificates, in which the CRL endpoint is a necessary attribute. Digipoort PI follows a soft fail approach where the service continues even if the CRL endpoint is not detected in the certificate. This is a trade-off between performance and security of Digipoort PI, based on the trust in the certificate hierarchy. With respect to scenario (d), Digipoort PI does not use an OCSP, but checks an offline CRL which is downloaded every 4 hours from the respective CSPs. This reduces the time span of a revoked certificate going undetected while communicating with Digipoort PI to a maximum of 4 hours. The scenarios we discussed above can be possible due to the recklessness of CSPs. Some of these scenarios have already been played out in the real world in the incidents related to Diginotar, Comodo and Turktrust in 2011, VeriSign in 2001 etc. The CSP recklessness can cause exposure of information flowing through Digipoort PI and in the case of incidents like DigiNotar a complete revoking and reissuing of the digital certificates. However no direct attack on the private key of Digipoort PI is possible due to this as it is generated and securely stored in the server by VENDOR1. Based on our findings in Table 20, the controls and measures taken post DigiNotar have also greatly improved the Dutch PKI. We therefore conclude that the exposure for the *Key Management* asset of Digipoort PI due to recklessness from existing CSPs is very low.

Table 20: CSP - Controls & Exposures for Key Management Asset

Threat Agent	Attack Scenarios	Minimum Controls Required	Existing Controls	Possible Exposures
CSP	a) The private key of a CSP is compromised due to lack of minimum security controls like strong passwords, or an anti-virus on the cryptographic modules of the CSP. All the certificates issued by the CSP and signed with their private key therefore cannot be trusted anymore. The certificates of Digipoort PI were also issued by the same CSP. The certificates and keys of Digipoort PI therefore cannot be trusted anymore and all have to be revoked and replaced leading to considerable business impact. b) Digipoort PI signed its certificates with a CSP. The CSP erroneously issues intermediate CA certificates to an entity, but were meant to be user	<u>Program of Requirements</u> a) CSPs should undergo strict certification procedures before they can issue PKIOverheid certificates. b) Infrastructures of the CSPs should be audited regularly. c) There should be controls to minimize down time due to the unavailability of a CSP. d) Incidents at the CSPs should be reported promptly and systematically. e) The CRL end point should be compulsorily mentioned on the digital certificates, by using a template in accordance with the Program of	a) CSPs meet rigid PKI-government requirements regarding their operational processes, technical resources, information security, expertise, reliability of staff and information supply to their audience. This is called the Program of Requirements (PoR). b) CSPs must submit a proof of conformity to the requirements periodically. A Policy Authority (PA) of the PKI-government monitors the CSPs regularly using penetration tests, external audits, and visiting the CSPs for checks. The PA function is performed by the PKIOverheid department of Logius. c) Digipoort PI has a	Strong controls are in place to mitigate the attacks, therefore the exposure is low. The failure to implement these controls properly can lead to exposures.

Threat Agent	Attack Scenarios	Minimum Controls Required	Existing Controls	Possible Exposures
	certificates. An attacker uses the intermediate certificate to generate rogue certificates. The rogue certificates could have been used to communicate with Digipoort PI. This causes exposure of the information flow through Digipoort PI. Moreover, this leads to damage to the key management asset of Digipoort PI because the certificates issued by the CSP cannot be trusted anymore leading to revoking of the certificates and considerable business impact. c) The Certificate Revocation List (CRL) of the CSPs lets Digipoort PI know which certificates are revoked. In this case the CSP did not include a link to the CRL location for revocation checking in the user certificates. Digipoort PI continues to communicate with a revoked certificate, leading to possible exposure of information from Digipoort PI. d) The Online Certificate Service Protocol (OCSP) is not maintained properly by the CSP. The OCSP is used by services to access the CRL in real time. Due to this the updated CRL list cannot be accessed in real time by the key management system of Digipoort PI. This leads to wrongful authentication of users with revoked certificates, and possible exposure of information flowing through Digipoort PI.	Requirements for the digital certificates issued. f) CRLs should be published by the CSPs in accordance with the Program of Requirements.	primary certificate and a backup certificate. If the primary certificate is compromised, the back-up certificate is used to ensure continuity. d) The Dutch government's policy legislation for CSPs mandates them to notify the Authority for Consumer and Market (ACM) and National Cyber Security Center (NCSC) when they are breached. e) Certificates are issued by the CSPs based on a template issued by the PoR which mandates the presence of a CRL end point on every certificate issued. f) CRLs are published according to the PoR and the revocation status information is refreshed once every 4 hours by the CSPs.	

- *Employees at Logius (Reckless, Errors, Disgruntled)*
  We realized earlier that the Certificate Manager at Logius performs the role of purchasing the certificates from the CSP. However she/he does not have any physical or logical access to the *private key* of Digipoort PI, as it is generated, stored and managed by VENDOR1 as the software supplier of Digipoort PI. Table 21 shows the attack scenarios, controls and exposures due to the employees at Logius on the *Key Management* asset.

  The scenarios (a) and (b) demonstrating the recklessness of a Certificate Manager are unlikely due to the existing controls shown in the table. The ordering of the certificate is a systematic process that is initiated by a service manager through DigiInkoop. The Certificate Manager has to follow strict procedures requiring approvals at multiple stages from managers. The responsibility for downloading the CER files from the CSP certificate stores lies entirely on the Certificate Managers. All the important documents related to the certificates are also password protected and is under the sole responsibility of the Certificate Manager and cannot be shared with any other employees. In addition to this, the certificate managers also undergo trainings in ISO and other internal information security trainings at the Belastingdienst academy which makes them aware of the risks of reckless behaviour. Based on the above findings we conclude that the exposure for the *Key Management* asset due to recklessness of employees at Logius is low.

  We enquired about errors in the certificate ordering process with the Incident Manager - Logius_Expert4 (Interview set 2 - Appendix IV). In a related incident several wrong CER files were issued by a CSP for Digipoort PI leading to revocation of those certificates and reissuing of new certificates with some additional costs for the reissued certificates. The incident was a result of errors made by VENDOR1 and Logius. VENDOR1 generated incorrect CSR files which were overlooked by the Certificate Manager during the filing. If the error had been detected before the CSR's were filed the Certificate Manager could have requested VENDOR1 to correct the mistake. The threat scenario (d) is similar to this incident and is therefore likely. It however does not lead to the exposure of any private key information. After the incident, the Certificate Managers are more careful in checking the CSRs before filing it. Both Certificate Managers and VENDOR1 use tools like *Networking4all* to check for correctness of the CSR (Networking4all, 2015). The threat scenario (c) can lead to the exposure of the CER file with the public key. The impact of this exposure is low because the CER contains the public key and the public key is not confidential. If such an error happens, the certificate can be easily revoked by the Certificate Manager. We therefore conclude that attacks due to errors by Logius employees are likely. The consequences of such errors can lead to revocation of the certificates. However, the exposure to the *Key Management* asset due to these attacks is low because of the existing controls.

  For the disgruntled employees, in the threat scenarios (e), (g) and (h) the disgruntled Certificate Manager exposes the information in the CER file. The CER file obtained from the CSP is the signed public certificate of Digipoort PI. A public certificate is meant to be public and therefore the impact due to a disgruntled employee revealing the CER file is low. In addition to this, a public key also cannot be implemented by an external entity without the corresponding private

key. Therefore the scenarios (e) and (h) can be considered unlikely in the case of the PKI of Digipoort PI. The above mentioned reasons and the revocation of all privileges and accounts of a departing Certificate Manager when she/he leaves Logius, makes the scenario (g) unlikely too. In scenario (f) the disgruntled employee alters the CER file before sending them to VENDOR1. If VENDOR1 installs the certificate in the production server of Digipoort PI, the certificates will fail in production. However VENDOR1 controls this by checking the hash values of the public key before and after the certification. This means that a disgruntled Certificate Manager cannot attack the *Key Management* asset of Digipoort PI by altering the CER file. The Certificate Manager also has no access to the private key of Digipoort PI. The controls like background screening of employees, confidentiality agreements, and training of employees also help in preventing disgruntlement. Therefore we conclude that the exposure due to a disgruntled employee at Logius on the *Key Management* asset is low.

Table 21: Logius Employees - Controls & Exposures for Key Management System

Threat Agent	Attack Scenarios	Minimum Controls Required	Existing Controls	Possible Exposures
Employee Reckless - Logius	a) The Certificate Manager should authenticate himself using a username and password to log into the portal of the CSP from where he can download the CER files. The CER file contains the public key information of Digipoort PI signed by the CSP. While in his absence, he gives his credentials to employee X who is not a Certificate Manager to download the CER files on his behalf. Employee X uses the Certificate Manager's credentials to download the CER files. She/he now has unauthorized access to the files which contain information about the public key of Digipoort PI. This could lead to exposure of the public key information. b) The Certificate Manager should authenticate himself using a username and password to log into the web portal of the CSP from where he can download the CER files. The CER file contains the public key information of Digipoort PI signed by the CSP. He downloads a CER file to send it to the supplier	ISO 27001/27002; BIR; ISO 9001 a) Proper Management of physical media to prevent disclosure of information. b) Documented operating procedures should be available for all users. c) Rules for acceptable use of assets are well documented. d) Confidentiality or non-disclosure agreements depending on the type of information being handled. e) Awareness and training for employees. f) Logging and monitoring of events to generate evidence. g) Strong access control policy for the document management system.	Media management a) Media assets are managed according to Logius standards. Information Handling b) Security policy and measures for handling confidential information is documented. Acceptable use of assets c) The Model Code of Conduct for government employees is documented in the 'Modelgedragscode Integriteit sector Rijk' and applies to Logius employees too. Confidentiality agreements d) Employees are made to enter into confidentiality agreements as part of the contract. Employee trainings e) Certification Manager is ISO 27001 certified. Training sessions on information security are conducted for employees by the	Low exposure due to the existing controls and also because the information contained in the CER file is public. Recklessness of Logius employees does not affect the private key in any way.

	(VENDOR1) for installing the certificate in the Digipoort server. The file is sent to the supplier via email. He uses his personal email id for sending the CER file to save time. This could lead to exposure of the public key information.		information security team. There are also internal trainings on information security from the Belastingdienst academy. Logging and Monitoring f) The ordering of the certificates is initiated by the Service Manager in DigiInkoop. The KD (Certificate Manager) then follows a series of steps in ordering the certificates. g) The CSRs to be filed are monitored using a CSR control process, usually performed by one of the other Certificate Managers. Document Management h) A strict username and password protection is used to download the CER from the CSPs. CSPs like QuoVadis also requires a token key to be entered while authenticating the Certificate Manager.	
Employee Error - Logius	c) The Certificate Manager should authenticate himself using a username and password to log into the portal of the CSP from where he can download the CER files. The CER file contains the public key information of Digipoort PI signed by the CSP. He downloads a CER file to send it to the supplier (VENDOR1) for installing the certificate in the Digipoort server. The file is sent to the supplier via email. He unknowingly sends the CER file to a person outside the Logius network. d) The Certificate Manager receives a CSR from VENDOR1 which is not correct. He applies for the	ISO 27001/27002; BIR; ISO 9001 a) Awareness and training for employees. b) Rules for acceptable use of assets are well documented. c) Strong access control policy for the document management system. d) Systematic error reporting is implemented. e) The certificate ordering process is systematic and monitored.	Employee training a) Training sessions on information security are conducted for employees by the information security team. Acceptable use of assets b) The Model Code of Conduct for government employees is documented in the 'Modelgedragscode Integriteit sector Rijk' and applies to Logius employees too. Document Management c) A strict username and password protection is used to download the CER from the CSPs.	Low exposure due to the existing controls and also because the information contained in the CER file is public. Errors made by Logius employees do not affect the private key in any way.

	certificate to the CSP without realizing the error in CSR. The CER file is created with the wrong CSR. The CER file is sent by the Certificate Manager to VENDOR1, which is then installed in the Digipoort PI server. However, the Digipoort service fails in production due to the incompatible certificate and the public-private key pair.		CSPs like QuoVadis also requires a token key to be entered while authenticating the Certificate Manager. Error Reporting d) An error made in the CER is reported first to the team leader of KD who then investigates it. The PKIOverheid and the Information Security department of Logius are also informed. Certificate Ordering e) The ordering of the certificates is initiated by the Service Manager in DigiInkoop. The KD (Certificate Manager) then follows a series of steps in ordering the certificates. Checks for CSR CSR Verification is done by the Certificate Manager and VENDOR1 using online tools like NETWORKING4ALL.	
Disgruntled Employee - Logius	e) The Certificate Manager at Logius is disgruntled due to some personal grudges with the organization. He takes revenge by logging into the portals of CSPs and downloading the CER files of Digipoort certificates. The CER file contains the public key information of Digipoort PI signed by the CSP. He then knowingly sends the CER files outside the Diginetwerk to external parties, causing exposure of the public keys. f) The Certificate Manager at Logius is disgruntled due to some personal grudges with the organization. He takes revenge by logging into the CSP portals and downloading the CER files of Digipoort certificates. The CER file contains the public key information of Digipoort PI	ISO 27001/27002; BIR; ISO 9001 a) Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized modifications or misuse of the information. b) Proper background verification of employees shall be carried out in accordance with relevant laws and regulations. c) Contractual agreements with employees for information security. d) Awareness and training for employees.	Control of separation a) Different departments within Logius are responsible for different parts of Digipoort, reducing the chances for unauthorized modifications or misuse of information. KD is responsible for the software layer and MS is responsible for the platform and infrastructure layer of Digipoort PI. Background checks b) A certificate of good conduct (VOG) is required for every employee before joining Logius. Confidentiality agreements c) Employees are made	Low exposure due to the existing controls and also because the information contained in the CER file is public. A disgruntled employee at Logius cannot attack the private key of Digipoort PI.

	signed by the CSP. He alters the CER files before sending it to the supplier (VENDOR1). g) The Certificate Manager at Logius is disgruntled due to some personal grudges. He resigns from Logius, but still accesses the CER files from the CSP certificate stores online using his credentials. He misuses the CER files by exposing the CSP signed certificate to external entities. h) The Certificate Manager at Logius is disgruntled due to some personal grudges. He resigns from Logius, but sends several CER files he downloaded using his credentials to his personal email id before leaving. He plans to expose the information in the CER files to external parties. The public keys along with other details about Logius are exposed.	e) Strong access control policy for the document management system. f) Disciplinary process against employees who have committed a breach. g) Proper definition of duties during termination of employment. h) Logging and monitoring of events to generate evidence.	to enter into confidentiality agreements as part of the contract. <u>Employee trainings</u> d) Certification Manager is ISO 27001 certified. Training sessions on information security are conducted for employees by the information security team. There are also internal trainings on information security from the Belastingdienst academy. <u>Document Management</u> e) A strict username and password protection is used to download the CER from the CSPs. CSPs like QuoVadis also requires a token key to be entered while authenticating the Certificate Manager. <u>Disciplinary process and termination of employees</u> f) When the Certificate Manager leaves Logius, all the CSPs are informed about this and the account is revoked. The team leader also ensures that the permissions within the Logius network are revoked and the responsible people at PKIOverheid are informed. <u>Logging and Monitoring</u> f) The ordering of the certificates is initiated by the Service Manager in DigiInkoop. The KD (Certificate Manager) then follows a series of systematic steps in ordering the certificates. <u>Hash Check for CER</u>

		VENDOR1 checks the hash value of the certificate to ensure that the certificate has not been altered by someone during the certification process.

- *Vendor*

  Table 22 shows the controls and exposures for the *Key Management* asset due to the vendor threat agents. According to Logius_Expert5 from VENDOR1 (Interview set 2 - Appendix IV) the scenarios (a) and (b) are unlikely due to the security policies of VENDOR1. Employees, especially administrators are not allowed to share or write down their passwords. Violating these policies could lead to the firing of the employee. Moreover, employees at VENDOR1 are trained to be aware about the risks of non-compliance to information security standards. This makes a Social Engineering attack on the employees difficult to execute. The scenario (c) is unlikely due to the highly secure infrastructure in which the VENDOR2 datacenters are housed. The authentication methods used in the data center include password verification, security keys and palm scanning. It is therefore unlikely for an unauthorized person to get access to the servers. The scenario (d) deals with the unavailability of the *Key Management* asset. We discussed earlier how an error in the CSR generated by VENDOR1 led to the revoking of several certificates. If the invalid certificates created due to that error were installed in the server by VENDOR1, it would have caused the asset to fail in production. However, this is an unlikely scenario because VENDOR1 checks the CER file for correctness before the certificate is installed in the server. In addition to this, VENDOR1 also maintains a primary and a back-up certificate in order to ensure continuity of the PKI. If the primary certificate fails due to an unexpected error, the back-up certificate is used to ensure the availability of the asset. The primary certificate of Digipoort PI is issued by KPN and the back-up certificate is issued by QuoVadis. Based on the above findings we conclude that there are sufficient controls to prevent any exposure to the key management asset due to the reckless behaviour of vendors.

  The threat scenarios (e), (f) and (g) discuss the hostile actions of a disgruntled administrator employee at VENDOR1 on the key management system. There are existing controls implemented by VENDOR1 to mitigate these kinds of attacks on the private key. Employee activities on the servers and databases are monitored and logged. There are also multiple administrators for the key server to ensure that no one administrator is completely in charge. Scenario (g) is unlikely because any change in the server like removal of an anti-virus by an administrator will be easily noticed by other administrators or users. Administrators are also required to follow a strict change management process requiring prior risk analysis of the change and approvals from the KD. In scenarios (e) and (f) the administrator compromises the private key of Digipoort PI by giving his access credentials to the key server, and exposing the private key itself to an external attacker respectively. Barring the difficulty for an external attacker to remotely access the key server of Digipoort PI in scenario (e), both scenarios (e) and (f) can be a likely attack method on the private key of Digipoort PI. This is because of the

administrators' high access to the server in which the private key is stored. However, the existing controls on Digipoort PI like logging and monitoring of employee activities on the key server and databases certainly reduce the exposure of the private keys of Digipoort PI to such an attack.

The scenario (h) is unlikely because the private key is stored very securely in the server and access to it is restricted to the administrators. A non-administrator employee (for instance a developer) only has limited pseudo-rights to the server in which the private key is stored. Therefore a disgruntled employee without administrator access will not be able to easily attack the private key of Digipoort PI without being detected. To prevent scenario (i) VENDOR1 immediately revokes all the accesses and administrator accounts (if any) of employees leaving the company to prevent unauthorized access. Scenarios (j) and (k) are also highly unlikely due to the high level of security in which the datacenters of VENDOR2 are maintained. Any unauthorized physical access or damage to the key servers of Digipoort PI is therefore highly unlikely.

Table 22: Vendor - Controls & Exposures for Key Management System

Threat Agent	Examples of Attack Method Description	Minimum Controls Required	Existing Controls	Possible Exposures
Vendor Reckless	a) Mr. X is an administrator at VENDOR1. He wrote down the password to the key server on a piece of paper for convenience. The paper wasn't shredded and ended up in the dumpster. A dumpster diving actor obtains the access credentials to the key server as a result. This could lead to the compromise of the key server and exposure of the private key. b) Mr. X is an employee of VENDOR1. A social engineering attacker tricks Mr. X into using a malware affected USB stick on the computer connected to the key server. The malware compromises the server and leads to exposure of the private key of Digipoort PI. c) An employee at VENDOR2 accidentally lets an unauthorized person tailgate into the building	ISO 27001/27002; BIR; ISO 9001 a) Separation of development, testing and operational environments. b) Monitoring and review of supplier services. c) Development lifecycle of information systems should be strictly followed. d) Strong access management to the server and its hardware. e) Awareness and training for employees. f) Redundancy of assets is maintained to ensure continuity.	Control of separation a) Development, testing and production environments are separated along with strict access control policies. Monitoring of services b) Monitoring and review of vendor activities are performed by the Keteninformatiediensten based on ITIL standards. Development lifecycle c) Logius is BIR compliant and therefore follows development lifecycle for information systems. Access Management to Server Hardware d) VENDOR2 employs the strongest access management and perimeter controls to their datacenters like password security, keys, hand scanning etc. e) At VENDOR1, there	Reckless behavior can lead to error in creation of certificates. However, the existing controls ensure that the exposures due to reckless behavior are low.

	where the key server is housed. The person accesses the server and manages to steal the private key from the server. d) An error in the server led to the generation of an incorrect CSR. The error was overlooked during validation and the CSR was sent to the Certificate Manager at Logius for certificate creation. The Certificate Manager sends the CSR to a CSP who creates an invalid certificate with the CSR. The CER file generated is downloaded by the Certificate Manager from the CSP certificate store and sent to VENDOR1 for installation in the server. VENDOR1 installs the public certificate (CER file) in the server. While in production, the TLS connections with clients fail because of the invalid public certificate. This causes unavailability of the key management system and the Digipoort PI service.		are at least two administrators who can access the key management system. This is for security purposes and also to ensure that no one person is fully in control of the asset. The access list of administrators is also handled by the Managed Services department of Logius. f) Vendors are mandated to be ISO certified and therefore perform suitable access management to the software and hardware assets. VENDOR1 and VENDOR2 are ISO 9001 and ISO 27001 certified. <u>Employee trainings at vendors</u> g) VENDOR1 conducts risk awareness sessions for its employees. <u>Redundancy</u> h) VENDOR1 maintains two sets of certificates for Digipoort PI services. This ensures redundancy. If one certificate fails due to some error, the back-up certificate is used. The primary certificate is issued by KPN and the back-up certificate is issued by QuoVadis. <u>Checks for CSR</u> CSR Verification is done by the Certificate Manager and VENDOR1 using online tools like NETWORKING4ALL.	
Employee Disgruntled - Vendor	e) A disgruntled administrator at VENDOR1 has access to the server in which the private key of Digipoort PI is stored. He shares his access credential information with an external attacker. External attackers misuse	<u>ISO 27001/27002; BIR; ISO 9001</u> a) Screening & Background verification of vendor employees. b) Contractual agreements for	<u>Background checks</u> a) A certificate of good conduct (VOG) is required for every employee before joining Logius. <u>Confidentiality agreements</u>	Private keys of Digipoort PI are generated and stored securely in the VENDOR1 servers. Existing controls shows low exposures due to disgruntled employees at

	credentials to steal the private key stored in the server (possibly over the network). The key system is compromised and communications are insecure. Logius now has to revoke the certificates. VENDOR1 has to generate new keys and get new digital certificates from the CSP. f) A disgruntled administrator employee at VENDOR1 has access to the server in which the private key of Digipoort PI is stored. He knows the location of the PEM file on which the private key is stored. He copies the private key and shares it with an external attacker. The key system is compromised and communications are insecure. Logius now has to revoke the certificates. VENDOR1 has to generate new keys and get new digital certificates from the CSP. g) A disgruntled administrator at VENDOR1 disables the anti-virus application on the key server. The key server is now unprotected and could become vulnerable to external attackers. h) A disgruntled non-administrator employee at VENDOR1 breaks into the server in which the private key of Digipoort PI is stored. He finds and copies the private key and shares it with an external attacker. The key system is compromised and communications are insecure. Logius now has to revoke the certificates. VENDOR1 has to generate new keys and get new	information security. c) Restriction on changes to servers, databases and other assets. d) Disciplinary process against employees who have committed a breach. e) Awareness and training for employees in information security. f) Proper definition of duties during termination of employment. g) Proper logging and monitoring of employee activities. h) Strong access management to the key server and its hardware.	b) Employees of Vendors and the Vendor organizations are made to enter into confidentiality agreements as part of the contract. <u>Change management</u> c) Changes to servers and database are restricted based on strict protocols. Every change request to the system follows change management process. A risk analysis is conducted by VENDOR1 for the change request and is signed off by the KD. <u>Disciplinary process</u> d) Any breach of security policy can lead to an enquiry and automatic firing of the employee. <u>Employee trainings at vendors</u> e) VENDOR1 conducts risk awareness sessions for its employees. <u>Termination of employment</u> f) All the accesses and permissions of employees terminating their services are revoked and administrator accounts if any are deleted. <u>Logging & Monitoring</u> g) Employee activities in the servers and databases are monitored and logged. <u>Access Management to Server</u> j) VENDOR2 employs the strongest access management and perimeter controls to their datacenters like password security, keys, hand scanning etc.	VENDOR2. Disgruntled administrators at VENDOR1 with access to the private key can be a likely threat.

	digital certificates from the CSP. i) Former administrator employee at VENDOR1 is disgruntled. He shares his access credentials and details regarding the implementation and location of the keys of Digipoort PI in the server to an external entity .The attacker now clearly know where to look for in the server to copy, alter or damage the keys of Digipoort PI. j) A disgruntled employee at VENDOR2 walks into a server room where the key server of Digipoort PI is housed. He physically sabotages the server in which the private key of Digipoort PI is stored. The server could malfunction and become unavailable for performing the encryption or decryption functions for Digipoort PI. k) Administrator employee at VENDOR2 is disgruntled and shares confidential information like the make and type of server used for storing the private key of Digipoort PI to hostile actors. The hostile actors try to physically access the server in which the key is stored. This can jeopardize the security of the private key of Digipoort PI.	k) At VENDOR1, there are at least two administrators who can access the key management system. This is for security purposes and also to ensure that no one person is fully in control of the asset. The access list of administrators is also handled by the Managed Services department of Logius.

- *Internal Spy*

  Table 23 shows the threat scenarios, controls and exposures for the Key Management asset due to an Internal Spy. An internal spy is unlikely to use scenarios like (a) and (b) due to the high chances of detection (Scahill & Begley, 2015). VENDOR2 employs a high level of security in their datacenters and VENDOR1 trains its employees in threat risk awareness. Therefore trying to physically break into the server at VENDOR2 and coerce or blackmail administrators at VENDOR1 can cause the internal spy to be detected easily. In scenarios (c) and (d) the internal spy helps an external attacker eavesdrop on the communications of the administrators of the *key management* asset of Digipoort PI to gather information on the private key. The key heist

that happened with Gemalto in 2010 shows that this is a very likely scenario in real world (Scahill & Begley, 2015). However, both Diginetwerk of the Dutch government and VENDOR1 networks are closely and constantly monitored for vulnerabilities and security anomalies. It is therefore highly unlikely that an internal spy will be able to install any malicious snooping programs in the systems of Logius and VENDOR1. An administrator of the key servers as an internal spy as shown in scenario (e) is a completely different case. Such an attack will be extremely hard to detect due to their high access levels, technical proficiency and clandestine nature. The background checks before hiring employees, strong access management to the key servers with close monitoring of the administrators by the Managed Services (MS) department of Logius, and logging and monitoring of the employee activities in the servers and databases of Digipoort PI keeps the exposure of the *Key Management* asset to internal spies low.

Table 23: Internal Spy - Controls & Exposures for Key Management System

Threat Agent	Examples of Attack Method Description	Minimum Controls Required	Existing Controls	Possible Exposures
Internal Spy (Logius/Vendor)	a) An internal spy at VENDOR2 physically breaks into the server hardware where the private key of Digipoort PI is stored. He then steals the private key of Digipoort PI and sells it to an external attacker. b) An internal spy uses Social Engineering techniques (blackmails, bribes, coercion) on the administrators at VENDOR1 to get access to the server of Digipoort PI where the private key is stored. She/he then sells the private key to an external attacker. c) An internal spy in Logius compromises Diginetwerk by planting malware on several computers in Logius. This gives the spy agency access to the network communications. The	ISO 27001/27002; BIR; ISO 9001 a) Screening & Background verification of vendor employees. b) Use of confidentiality or non-disclosure agreements c) Restriction on changes to servers, databases and other assets. d) Strong access management to the key server and its hardware. e) Proper logging and monitoring of employee activities. f) Network monitoring and performance monitoring of the assets. g) Awareness and training for employees in information security.	Background checks a) A certificate of good conduct (VOG) is required for every employee before joining Logius. Confidentiality agreements b) Employees of Vendors and the Vendor organizations are made to enter into confidentiality agreements as part of the contract. Change management c) Changes to servers and database are restricted based on strict protocols. Every change request to the system follows change management process. A risk analysis is conducted by VENDOR1 for the change request and is signed off by the KD. Access Management to Server j) VENDOR2 employs the strongest access management and perimeter controls to	Administrators as internal spies can attack the private keys of Digipoort PI. Constant monitoring of administrator activities by MS, background checks, and logging and monitoring of administrator activities keeps the exposure of Digipoort PI to the internal spy threat agents low.

	spies are able to monitor the communications of the administrators of the key management system. They compromise the email account of a Certificate Manager of Digipoort PI and steal the CER file sent to VENDOR1. The CER file contains information regarding the public key of Digipoort PI. d) An internal spy in VENDOR1 compromises the VENDOR1 network by planting malware on several computers in VENDOR1. This gives the spy agency access to the network communications. The spies are able to monitor the communications of the administrators of the key management system. They spy on the details regarding the location of the private key and the access credentials to the server in which it is stored. The private key is stolen by accessing the servers using the information collected. e) An administrator employee at VENDOR1 is an internal spy. He knows the location of the PEM file on which the private key is stored. He copies the private key and sells it to an external attacker for money. The key system is compromised and communications are	their datacenters like password security, keys, hand scanning etc. k) At VENDOR1, there are at least two administrators who can access the key management system. This is for security purposes and also to ensure that no one person is fully in control of the asset. The access list of administrators is also handled by the Managed Services department of Logius. <u>Logging & Monitoring</u> g) Employee activities in the servers and databases are monitored and logged. <u>Network & Infrastructure Monitoring</u> h) The Diginetwerk is monitored 24 hours per day, and 7 days a week for any observed disturbances in the network. i) VENDOR1 monitors the Digipoort PI IT infrastructure and network using the NAGIOS open source computer software application. NAGIOS offers monitoring and alerting services for servers, switches, applications and services. <u>Employee trainings at vendors</u> e) VENDOR1 conducts risk awareness sessions for its employees.

	insecure. Logius now has to revoke the certificates. VENDOR1 has to generate new keys and get new digital certificates from the CSP.	

Threat Landscape – Key Management Asset of Digipoort PI

If we recall our conceptualization of a threat landscape in Chapter 5, we realize that the TARA methodology we applied to the PKI of Digipoort PI above has helped us in understanding the attributes, the methods of attack and objectives of the threat agents relevant to it. Furthermore, we also discussed the controls and exposures in Digipoort PI to certain sample attack scenarios associated with the threat agents and the *Key Management* asset of Digipoort PI.

Based on the analysis we conducted earlier, we realized that *Reckless End Users* cannot attack the PKI of Digipoort PI. A compromise in the private key of a company connecting to Digipoort PI will make the TLS connection between that company and Digipoort insecure. However, it does not cause any damage to the private key or the PKI of Digipoort PI. Similarly reckless actions of a *CSP* could lead to the compromise of its own private key, but with no serious exposure to the private key of Digipoort PI. Due to the hierarchy of trust in the PKI, certificates that are obtained from that particular CSP by Digipoort PI will become invalid and have to be revoked and replaced. The DigiNotar incident was a testimony to this. Incidents like DigiNotar leads to considerable business impact because of the loss of continuity in e-government services using the PKI. Digipoort PI and other services of Logius are now equipped with back-up certificates to ensure continuity of the service in case of such unexpected adversities. Nonetheless, there will always be a residual risk associated with CSPs as a threat agent due to its high impact on the PKI of Digipoort PI (Dijk, Konen, & Svartz, 2014).

Employees of Logius do not have any physical or logical access to the PKI of Digipoort PI. The only point of contact for VENDOR1 in Logius regarding the certificates is the Certificate Manager of Logius. Based on the analysis we conducted earlier, we conclude that a Certificate Manager cannot attack the private key of Digipoort PI. The recklessness of a Certificate Manager can lead to exposure of the CER file, but there is no big impact because the information contained in the CER file is public. Errors made by the Certification Manager in filing the CSR could lead to the issuance of a wrong CER file by the CSP and unavailability of the PKI of Digipoort PI. A disgruntled Certification Manager can also cause unavailability by altering the contents of the CER file being sent to VENDOR1. However these attacks are mitigated by the redundancy of the certificates, and the CSR checks and hash checks VENDOR1 does before installing the certificates in the servers.

Vendors are the most important threat agent with respect to the *Key Management* asset of Digipoort PI. The private and public keys are generated by administrators at VENDOR1 in the servers of Digipoort PI.

The private key is stored securely in the servers. A disgruntled administrator at VENDOR1 can attack the private key of Digipoort PI by giving his access credentials to an external attacker or exposing the private key itself. The existing controls in Digipoort PI however show that there is no vulnerability due to this threat agent. A disgruntled employee at VENDOR2 cannot attack the private key because of the highly secure environment in which the servers are maintained. Reckless behaviour like misuse of passwords by administrators at VENDOR1 is not likely. Error in the generation of CSRs by VENDOR1 is likely. This can lead to the issuance of wrong certificates by the CSP. Unavailability of the PKI due to these errors is mitigated by the redundancy of the certificates.

Internal Spies at vendors can be of higher risk than internal spies at Logius because of their possible physical and logical access to the *Key Management* asset. An internal spy at VENDOR1 with administrator access can attack the key server to extract the private key of Digipoort PI. However, the background checks before hiring employees, strong access management to the key servers with close monitoring of the administrators by the Managed Services (MS) department of Logius, and logging and monitoring of the employee activities in the servers and databases of Digipoort PI makes the likelihood of this attack low. Without administrator access an internal spy can also attack by eavesdropping on the communications of administrators. This is however less likely due to the difficulty in compromising the networks of VENDOR1 or the Diginetwerk itself.

Above we summarized the threat landscape of the *Key Management System* of Digipoort PI by applying the TARA methodology using the tailored TAL and MOL artifacts we created in Chapter 6. Based on the similarity of implementation of the PKI in Digipoort PI and Digipoort OTP, we infer that the results of this analysis are also applicable to the *Key Management* asset of Digipoort OTP

7.4. Reflection & Learning from Application

In this section we reflect on the tailored TAL and MOL artifacts, the TARA methodology and the results of their application on the *Key Management System* of Digipoort PI. We applied the tailored TAL and MOL on a critical asset of Digipoort PI using the TARA methodology. In this way we were able to understand the threat landscape of that critical asset. Understanding the threat landscape of Digipoort PI needs the comprehensive evaluation of all the important assets of Digipoort PI. Based on the TARA methodology we used, it is possible to understand the threat landscapes for the other assets of Digipoort PI too as shown in Appendix V. This is however not without difficulties. While applying the methodology we required inputs from internal experts in the form of interviews to identify critical assets, relevant threat agents, and develop threat scenarios for the assets. This shows that the even though the tailored TAL and MOL promises a certain level of innate knowledge in the form of pre-defined threat agent characteristics, the methodology still requires a considerable amount of external inputs to produce results. This cannot be considered as a limitation of the methodology. Time constraints and the limited knowledge of the researcher also could have played a role in this.

Flexibility to time constraints and ease of use for non-expert users were two non-functional requirements used in the selection of the TARA methodology from state of the art in Chapter 5. We do not have any empirical validation with respect to these requirements. However, the ability of the

methodology to be applied to selected assets, using a prioritized list of threat agents, and generate results about the threat landscape shows that the methodology is flexible and adaptable to time constraints. Also, as a non-expert user we could execute the methodology by using interview data, data from literature and technical artifacts available at Logius. This in a way justifies the selection of TARA methodology for this research.

In the application of the methodology, we prioritized the threat agents based on the relevance scores that the expert on Digipoort PI gave to each threat agent. This type of prioritization was performed because of the lack of a baseline risk level to prioritize the threat agents. In future iterations, the threat agents should be prioritized according to the baseline risk level set by security experts based on threat intelligence data. In any case, the prioritization of threat agents does not mean that the low priority threat agents are ignored. Instead it makes the analysis more manageable by focusing on the most important threat agents. This is an inherent advantage of TARA. As Rosenquist (2009) puts it - TARA does not attempt to identify every single weak point, TARA methodology identifies the risks of greatest concern. However in this application we still needed to make sure that no threat agents were wrongly prioritized. We did this by proactively questioning the interviewer's relevance scores based on threat agent attributes and methods.

Furthermore, the absence of CEL made us build threat scenarios to identify vulnerabilities and exposures. Although effective, building threat scenarios require considerable knowledge about the asset and the threat agents. Practitioners of the methodology should focus on building a CEL when enough knowledge has been created from the iterations of the methodology. This will lend more structure and efficiency in the application of the methodology.

Ultimately the threat intelligence we derive by applying the TARA methodology will be based on the tailored TAL and MOL artifacts we created. Therefore the comprehensiveness and correctness of TAL and MOL will determine the quality of the threat landscape created from the methodology. The comprehensiveness of the library depends on the information available at our disposal for creating the library. Let us take the case of the *Terrorist* threat agent that does not feature in our library. This could be because this threat agent is not very relevant for the infrastructure (Digipoort) we analyzed or because the last 5 years of incidents we analyzed did not feature such an extreme attack. Either way, the threat agent is not included because it is not one of the most relevant at this point of time. The landscape might change in the future and extreme attacks on such infrastructures might become more relevant. In such a case the flexibility of TAL will enable the easy addition of the *Terrorist* threat agent to the library if necessary. Determining the characteristics of threat agents with correctness is also not easy. We determined most of the threat agent characteristics from information security literature and incident data, supplemented with interview data of cyber risk experts. This was neither efficient nor easy as we had to examine a large number of literatures that often differed in quality and structure, to identify individual attributes. Therefore the identification of the attributes, methods and objectives of the threat agents were not linear, but involved multiple iterations of the TAL and MOL artifact. This is however not explicitly depicted in the BIE phase of our ADR model. We also tried to support our arguments from literature with practical incidents related to the threat agents wherever possible. This lends some accuracy to the artifacts we designed. The results of the application do not validate the

comprehensiveness or accuracy of the artifacts, but shows their usability in understanding the threat landscape of e-government infrastructure for businesses.

7.5. Summary

In this chapter we answered the fourth research sub-question, "*What are the results of applying the tailored threat agent centric threat assessment methodology in a practical case study?"* To answer this sub-question, we used the tailored TAL and MOL artifacts for e-government infrastructure for businesses to perform a minimal version of the TARA methodology (shown in Figure 25) to the *Key Management System* of Digipoort PI. A broader version of the TARA methodology covering the other assets of Digipoort PI is also shown in Appendix V. In Step 1 we used a TAL based questionnaire to interview an expert in Digipoort PI to prioritize the threat agents and identify the critical assets for Digipoort PI. We also identified the likely methods and objectives of the relevant threat agents from the tailored MOL as shown in Table 18. The *Key Management System* was selected as the critical asset for our analysis based on the outputs from Step 1. We focused our analysis on the prioritized list of threat agents as shown in Table 17. Further in Step 2 we devised sample attack scenarios for each threat agent based on their likely methods of attack. We also identified the minimum controls required and existing controls in the *Key Management* asset to mitigate the attacks.

Based on our findings we analyzed the exposures for the *Key Management* asset by comparing the minimum and existing controls as shown in tables 19 to 23. Subsequently we concluded that threat agents like End User Recklessness, CSPs, Employees at Logius, and Vendor Recklessness cannot attack the PKI of Digipoort PI due to the existing controls in Digipoort PI and the PKI in general. A disgruntled employee at VENDOR1 with administrator access or an internal spy at VENDOR1 with administrator access can attack the PKI by sharing their credentials to external attackers or copying and exposing the private key from the server. However, we found enough evidence of mitigating controls in Digipoort PI against these threat agents which leads us to conclude that there are no serious exposures to the Key Management System of Digipoort PI due to these threat agents.

We applied the tailored TAL and MOL artifacts on Digipoort PI here as part of the *Reflection and Learning* phase of the ADR model. The application process and the results of the application of TARA on Digipoort PI helped us in reflecting and learning about the TARA methodology, the tailored TAL and MOL artifacts, and their designing in Chapter 6.

Conclusion

8. Conclusions

To formalize learning researchers need to outline the accomplishments realized in the IT artifact and describe the organizational outcomes (Sein et al., 2011). In this chapter we do this by drawing conclusions from the research and reflecting on them. In the *Problem Formulation* stage we realized that there was no clear definition for a 'Threat Landscape' in literature. We therefore defined a threat landscape as "the characteristics (attributes), the likely threat actions (methods), and objectives of the different types of threat agents who may act against the assets of an organization". Further, we also identified the lack of a systematic methodology for understanding the threat landscape of e-government infrastructures as the problem statement.

Based on the scope of our research the main objective was to use a threat assessment methodology to understand the threat landscape of e-government infrastructure for business enterprises. We achieved the objective of this research by answering the main research question, ***"How can a threat assessment methodology be used to understand the threat landscape of e-government infrastructure for businesses?"*** We used TARA methodology, a threat agent centric threat assessment methodology for understanding the threat landscape of e-government infrastructure for business enterprises. The main outputs of the question are ***the tailored TAL*** in Figure 23, and ***the tailored MOL*** in Figure 24 which are used to apply the TARA methodology for e-government infrastructure for business enterprises. We answered the four sub-questions pertaining to the main research question using the ADR model. We reflect on the answers to the sub-questions in the following section.

8.1. Reflection on Sub-Questions

In this section we discuss the knowledge we collected for each sub-question at the various stages of the research in order to answer the main research question.

SQ 1: *What are e-government infrastructures for businesses?*

The first sub-question was answered in the *Problem Formulation* stage, in Chapter 3 and Chapter 4 of the report. In Chapter 3 we defined e-government as the use of information and communication technologies to enable the daily administration activities of governments. The increasing complexity of e-government implementations restrict the use of generic architectures and enhance the need for security. The chapter reinforced the importance of understanding the threat landscape of e-government infrastructures. In Chapter 4 we described in detail a case of e-government infrastructure for business enterprises managed by Logius - Digipoort. We identified the two types of Digipoort namely Digipoort OTP and Digipoort PI. From the use cases of Digipoort OTP, we studied the interaction of the Digipoort system with various external actors like the reporting parties (businesses and intermediaries), government agencies, Vendors, and TTPs. Both the infrastructures perform the job of transferring information between businesses and governments, however using different technologies and interfaces. Web Services and PKI are important enabling technologies used by Digipoort. While Web Services are used only by Digipoort PI for providing various services to businesses and governments, the PKI is used

both by Digipoort OTP and Digipoort PI for ensuring the confidentiality, integrity and non-repudiation of Digipoort.

SQ 2: *What is the state of the art in threat assessment methodologies for e-government infrastructures?*

The second sub-question was also answered in the *Problem Formulation* stage, in Chapter 5 of the report. The literature review showed three different types of threat assessment methodologies - software centric, asset centric and threat agent centric. We discussed software centric methodologies like Microsoft SDL Threat Modeling Tool, asset centric methodologies like Threat Assessment Model for Electronic Payment Systems (TAME) and Cyber Threat Susceptibility Assessment (TSA), and threat agent centric methodologies like Operational Threat Assessment (OTA) & General Threat Matrix (GTM), and the Intel – Threat Agent Risk Assessment (TARA). We regarded the Intel TARA methodology to be more suitable for our research based on its focus on threat agents, ease of use, and flexibility in execution. Further we discussed the TARA methodology and the relevant libraries for research, the Threat Agent Library (TAL), and the Methods & Objectives Library (MOL) in detail. We also realized two limitations of the TARA methodology that needed to be overcome in order to apply the methodology to e-government infrastructure for business enterprises. First, the Intel TAL did not take into account all the threat agents that were relevant for e-government infrastructure for businesses. Second, the MOL was incomplete and had to be modified according to the TAL. The two limitations and how we dealt with them were discussed further in *BIE* phase, Chapter 6 of the report.

SQ 3: *How can a threat assessment methodology be adapted for e-government infrastructure for businesses?*

The third sub-question was answered in the *BIE* phase, in Chapter 6 of the report. In order to apply the threat agent centric threat assessment methodology to e-government infrastructure for businesses we addressed the two limitations of TARA methodology we realized in SQ 2. First, we tailored the Threat Agent Library (TAL) as shown in Figure 23 by adding threat agents that were relevant for e-government infrastructure for businesses. We analyzed the use cases of Digipoort OTP we developed in Chapter 4 and surveyed past incidents in the public sector to identify the threat agents to be added to the tailored TAL. Second, we tailored the Methods & Objectives Library (MOL) as shown in Figure 24 for the threat agents in the tailored TAL. By overcoming the two limitations we enabled the TARA methodology to be applied for e-government infrastructure for businesses. This is demonstrated in the application of the TARA methodology in Chapter 7.

SQ 4: *What are the results of applying the adapted threat assessment methodology in a practical case study?*

The fourth sub-question was answered in the *Reflection and Learning* phase, in Chapter 7 of the report. We applied the tailored TARA methodology to the *Key Management* asset of Digipoort PI in two steps as shown in Figure 25. In Step 1 we used a tailored TAL based questionnaire to identify the critical assets and relevant threat agents for Digipoort PI. We also identified the likely methods and objectives of the relevant threat agents from the tailored MOL. In Step 2 we created sample attack scenarios for the threat agents based on their likely methods of attack. We then identified the minimum security controls

and the existing controls in Digipoort PI against the sample threat scenarios. By comparing the minimum and existing controls we analyzed the exposures for Digipoort PI against the threat agents as shown in tables 19 to 23. Subsequently we summarized the threat landscape of the *Key Management* asset of Digipoort PI. Though not empirically validated, the learning from the application of the TARA methodology seems to justify our selection of TARA methodology for this research.

By answering the sub-questions we have shown how the threat landscape of e-government infrastructure for business enterprises can be understood using a threat assessment methodology. We concluded that a threat agent centric threat assessment methodology like TARA can be used for this purpose. We tailored the TAL and MOL artifacts of TARA methodology to adapt it for e-government infrastructure for businesses. We also demonstrated this by applying the methodology to the case of Digipoort PI. In this way we have met our research objective and answered the main research question. In the following sections we perform a reflection of the outcomes of the research and its limitations, followed by a discussion of the scientific and practical contributions of this research, and possibilities for future research in this area.

8.2. Reflection on Research

Threat Agent Centric Methodologies

A major conclusion from our research is that a threat agent centric threat assessment methodology like TARA can be used to understand the threat landscape of e-government infrastructures for businesses. However every threat agent centric threat assessment methodology might not be able to replicate similar results for threat landscapes like TARA. The main reason for this is the use of TAL and MOL in TARA. TAL and MOL provide assessors with libraries from which they can select threat agents that are uniquely defined based on their characteristics. For instance, another threat agent centric threat assessment methodology like the Operational Threat Assessment (OTA) methodology discussed in Chapter 5, focuses on creating a General Threat Matrix (GTM) based on the *Commitment* and *Resources* characteristics of a threat. Although this helps in characterizing and differentiating threats against targets of interest, obtaining the same level of knowledge about threats as in our definition of threat landscapes will require a lot of adaptation to the OTA methodology. Therefore it cannot be established that all threat agent centric threat assessment methodologies can be used to generate threat landscapes in the same level of detail as TARA.

Threat agent centric methodologies have their strengths and weaknesses. The main strength is that threat agent centric methodologies can be used in the proactive threat assessment of organizations. Especially in the case of TARA, the TAL and MOL libraries can be easily used to identify, predict and prioritize threats against infrastructures. This coupled with the ease of use, enables assessors to identify the most critical areas of exposure without having to identify every single weak point in the system. This will reduce the time and resources organizations spend in threat assessment by focusing on all the vulnerabilities. However, this also points to the weakness of agent centric methodologies. By focusing on threat agents, the assessor limits their scope to things that can go bad with the identified threat agents, and miss their focus on the asset value that organizations ultimately want to protect. In conclusion, an assessor using a threat agent centric methodology should always have a clear

understanding of the critical assets they are trying to protect, and should avoid randomly selecting threat agents based on their characteristics.

Extending TAL and MOL Further

The TAL and MOL libraries of TARA methodology we developed can be applied to e-government infrastructure for businesses, as demonstrated in Chapter 7. An important advantage of the TAL and MOL is that it is flexible enough to be extended and applied to e-government infrastructures for other domains, e-government infrastructures in other countries and infrastructures in other sectors. This will be possible by making suitable adjustments to the TAL and MOL artifacts. For instance applying the TAL and MOL we developed in the Government to Citizen (G2C) domain will require some minor modifications. The end user threat agent will change in this case from being represented as a business to a citizen. This means that their *Resource* attribute will change from *Organization* to *Individual* and the *Skills* attribute will change from *Adept* to *Minimal* or *None*. By similarly adjusting other threat agent attributes if necessary, the TAL and MOL artifacts can be adapted to the G2C domain.

Applying the TAL and MOL for an e-government infrastructure of a country other than the Netherlands, will require the adaptation of the artifacts to the specific e-government implementation of that country. From SQ 2 we realized that e-government implementations for countries differ based on a variety of factors including working cultures, skill sets, access to technology, and relevant infrastructure. However there can be similarities in implementations too. For instance an European eGovernment Services study reports that 14 out of the 32 countries studied uses public sector controlled PKI systems (Graux & Majava, 2007). In those cases the threat agents like CSP can be adapted easily. Therefore we believe that it will be easier to adapt the TAL and MOL artifacts to other countries if they have similar e-government implementations.

Furthermore, to apply the TAL and MOL artifacts to another sector will require the adaptation of the artifacts according to the characteristics of that sector. This is similar to what we have done in this research where we used inputs from the TAL in Figure 18 for Intel and in Figure 19 for the healthcare sector. This shows that the TAL and MOL artifacts we developed can be inputs for developing TAL and MOL for other sectors.

Limitations of Research

Every study has its limitations and it is really important to address them in foresight. The objectives and scope of our research also brings some limitations with it. One of the main limitations of the research is concerned with the selection of threat agents to be included in the tailored TAL for e-government infrastructures. We selected threat agents by analyzing the Digipoort OTP use cases and the past incident data in the public sector. Due to the constraints of our research we had to limit our analysis to only the use cases of Digipoort OTP and past incident data to the range of five years between 2015 and 2011. This limitation might have had some effect on the threat agents that we selected to be included in the tailored TAL. However, according to the Digipoort expert at Logius we interviewed (Interview Set 1 - Appendix IV) the list is fairly complete and can be successfully used for a threat landscape analysis of e-government infrastructure for businesses.

Another limitation is regarding the external and internal interviews we conducted. We interviewed two external security experts as shown in Appendix III. Due to the difficulty in finding suitable candidates from the public sector, we could only get the responses of two security experts. There were differences in the level of experience and the type of work being done by the experts. These factors might have influenced their responses which could have differed due to their differing exposure to security incidents and threat agents in the past. The interview we conducted with the expert on Digipoort PI as shown in Appendix IV also has its limitations. The expert's opinion could have had some biases depending upon his level of knowledge and his past experience in working with Digipoort PI. This could have been overcome by interviewing more experts in Digipoort PI. However the tight set up of the research did not provide the flexibility to do that, and there weren't many experts available in Logius to be interviewed regarding Digipoort PI.

Further, during the application of the tailored TAL and MOL using the TARA methodology in Chapter 7, we only took into account certain sample attack scenarios. An extensive threat analysis is beyond the scope and timelines of this report and therefore we had to rely on sample attack scenarios to demonstrate the application of the methodology. There were also administrative limitations which had to be taken into account with regards to getting appropriate documentation regarding the Digipoort infrastructure which led to a less extensive threat analysis. However, the main objective of the chapter was to demonstrate the application of the tailored TARA methodology and learn from it, which we successfully did.

Furthermore, decisions were made regarding the granularity of the threat agents in the tailored TAL. For instance, we decided to consider the threat agent archetypes, End User Recklessness and Vendor Recklessness but not End User Error and Vendor Error. But at the same time we made a differentiation between Employee Recklessness and Employee Error. This is because in the case of End Users and Vendors, we considered careless mistakes or errors as part of reckless behaviour and therefore did not split the threat agents into two archetypes to add more complexity to the list of threat agents. However in the case of employees the number of past incidents (Appendix II) related to errors made by employees were high enough to consider Employee Error as a separate threat agent archetype of employees. This limitation in a way also shows the flexibility of the methodology.

Finally, a more obvious limitation of the thesis is the lack of a systematic evaluation of the TAL and MOL artifacts created. Although the *BIE* phase of the research involved lot of reiterations of the artifact, due to the time constraints of the research, we could not demonstrate in a structured way the reiterations and the continuous evaluation of the TAL and MOL artifacts created.

8.3. Contributions

Here we describe the scientific and practical contribution of this research to the field of Information Security. The first two contributions below discuss the contributions of the research from a scientific perspective and the third one describes the practical contribution to the field.

1) *Defining a threat landscape.*

In the beginning of the research, we found many definitions for a threat landscape from literature. However, none of the definitions were concrete enough for developing a scientific approach towards understanding the threat landscape of organizations. So in Chapter 5 we conceptualized and defined a threat landscape as the combination of threat agents, their attributes, penetration methods, and objectives. This definition of threat landscape gives a more concrete idea of the concepts that should be studied to understand the threat landscape of organizations and their assets.

2) *Library for threat agents.*
During the course of this research, we have developed a library of threat agents for e-government infrastructure for businesses in the form of the tailored TAL and the associated tailored MOL. The library we developed can be used for understanding the threat landscape of e-government infrastructures as demonstrated in Chapter 7. A similar threat agent library for e-government domain does not exist in Information Security literatures to the best of our knowledge. Our work gives researchers wanting to understand the threat landscapes of e-government infrastructures, an easy starting point for threat assessment. The library of threat agents can also be extended in the future to modify, add or remove threat agents according to the domain of interest and the evolving cyber threats.

3) *Methodology for developing the threat landscape of organizations and IT infrastructures.*
In Chapter 7 we demonstrated how the TARA methodology can be used to develop the threat landscape of e-government infrastructure for business enterprises. The methodology makes use of the tailored TAL and tailored MOL to proactively create a snapshot of the threat agents relevant for the critical assets of an organization and its assets. It enables organizations to be aware of their critical assets, and its controls and exposures with respect to relevant threat agents in their domain. For instance, Logius can use the TARA methodology to understand the threat landscape of their e-government infrastructure for businesses like Digipoort OTP and DigiInkoop. With an extended library of threat agents, the methodology can also be applied for other e-government infrastructures like DigiD, MijnOverheid etc.

8.4. Future Research

The research on threat landscapes is comparatively new. As we realized from the state of the art in Chapter 5, most of the literature on threat assessment is still software centric and asset centric. This provides enough scope for future research on the topic.

We developed a library of threat agents and their methods and objectives for understanding the threat landscape of e-government infrastructure for business enterprises. There is scope for extending the library in the future depending on the change in the global cyber landscape and the requirements of the system under analysis. New agents can be added to the library or existing threat agents can be modified to fit the needs of the analysis.

In this research we focused mainly on the e-government domain, and especially on e-government infrastructures for business enterprises. This leaves room for the TAL, and the MOL in the TARA methodology to be extended for other infrastructures within e-governments or for entirely new sectors. We are already aware of the TAL developed by Houlding et al. (2012) for the health care sector. Similar libraries could be developed for other sectors too. There is also the possibility of building tools to

automate the methodology in the future. The TAL, the MOL could be built as online libraries to build the threat landscape of organizations. Regular threat landscape analysis could lead to a library of threat landscapes over a period of time which can then be used to study patterns of change in the threat landscapes of organizations and its assets.

Perfect security can be expensive or sometimes even an impossible goal to achieve (Fehr, 2011). By focusing on the threat agents who can attack the critical assets of an organization and by building controls to prevent those attacks, assessors can help in proactively mitigating the risks involved to a certain extent. Threat agent centric threat assessments enable organizations to do this in a resourceful manner. This research is a step forward in the area of threat agent centric threat assessments and holds more possibilities for future research in this area.

References

Abraham, D. G., Dolan, G. M., Double, G. P., & Stevens, J. V. (1991). Transaction Security System. *IBM Systems Journal*, *30*(2), 206–229. doi:10.1147/sj.302.0206

Barreira, I., Gustavsson, T., Wiesmaier, A., Galan, C., & Gorniak, S. (2013). *Mitigating the impact of security incidents*. *Guidelines for trust services providers – Part 3*. Athens, Greece.

Bateman, T. (2013). Police warning after drug traffickers' cyber-attack. Retrieved April 17, 2015, from http://www.bbc.com/news/world-europe-24539417

Bekkers, V. (2003). E-government and the emergence of virtual organizations in the public sector. *Information Polity*, *8*(3-4), 89–101.

Belanger, F., & Hiller, J. S. (2006). A framework for e-government: privacy implications. *Business Process Management Journal*, *12*, 48–60. doi:10.1108/14637150610643751

Bharosa, N., Wijk, R. van, Winne, N. de, & Janssen, M. F. W. H. A. (2015). *Challenging the Chain - Governing the Automated Exchange and Processing of Business Information*. *IOS Press under the imprint Delft University Press.* Delft. doi:10.3233/978-1-61499-497-8-i

Bharti, V. (2011). *Unified Cyber Security Monitoring and Management Framework*. Happiestminds - Bangalore. Retrieved from http://www.ten-inc.com/presentations/HappiestMinds-Unified-Cyber-Security-Monitoring.pdf

Bittner, K., & Spence, I. (2002). *Use Case Modeling*. Addison-Wesley Professional.

Bleikertz, S., Mastelić, T., Pieters, W., Pape, S., & Dimkov, T. (2013). Defining the cloud battlefield: Supporting security assessments by cloud customers. *Proceedings of the IEEE International Conference on Cloud Engineering, IC2E 2013*, 78–87. doi:10.1109/IC2E.2013.31

Bottom, N. R. (2000, June). The Human Face of Information Loss. *Security Management, Vol. 44, No. 6*. Retrieved from https://www.questia.com/read/1G1-63542481/the-human-face-of-information-loss

Brown, T. L., Potoski, M., & Van Slyke, D. M. (2006). Managing Public Service Contracts: Aligning Values, Institutions, and Markets. *Public Administration Review*, *66*(3), 323–331. doi:10.1111/j.1540-6210.2006.00590.x

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal*, *15*, 5–25. doi:10.1111/j.1365-2575.2005.00183.x

Casey, T. (2007). *Threat Agent Library Helps Identify Information Security Risks*. USA. Retrieved from https://communities.intel.com/docs/DOC-1151

Casey, T. (2015). *Understanding Cyberthreat Motivations to Improve Defense*. USA. Retrieved from http://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/understanding-cyberthreat-motivations-to-improve-defense-paper.html

Casey, T., Koeberl, P., & Vishik, C. (2010). Threat Agents : a Necessary Component of Threat Analysis. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (2010)*. doi:10.1145/1852666.1852728

Choo, K. K. R. (2011a). Cyber threat landscape faced by financial and insurance industry. *Trends and Issues in Crime and Criminal Justice*, (408).

Choo, K. K. R. (2011b). The cyber threat landscape: Challenges and future research directions. *Computers and Security*, *30*(8), 719–731. doi:10.1016/j.cose.2011.08.004

Choo, K.-K. R. (2014). A Conceptual Interdisciplinary Plug-and-Play Cyber Security Framework. In H. Kaur & X. Tao (Eds.), (pp. 81–99). London: Springer. doi:10.1007/978-1-4899-7439-6

Cotterman, W. W., & Kumar, K. (1989). User cube: a taxonomy of end users. *Communications of the ACM*, *32*(11), 1313–1320. doi:10.1145/68814.68816

Croall, H. (2001). *Understanding white collar crime*. *Open University Press*. United Kingdom: Open University Press. Retrieved from https://www.mheducation.co.uk/openup/chapters/0335204279.pdf

Danish, D. (2006). The Failure of E-Government in Developing Countries: A Literature Review. *The Electronic Journal of Information Systems in Developing Countries*, *26*(7), 1–10.

Digicert. (2015). Check our Numbers. Retrieved August 2, 2015, from https://www.digicert.com/TimeTravel/math.htm

Dijk, W. van, Konen, A., & Svartz, N. (2014). *International Case Report On Cyber Security Incidents*. Retrieved from https://www.gccs2015.com/sites/default/files/documents/ICR_CYBERCECURITYINCIDENTS_LR.PDF

DutchNews.nl. (2015a). Cyber attacks double on Dutch government websites. Retrieved August 20, 2015, from http://www.dutchnews.nl/news/archives/2015/08/cyber-attacks-double-on-dutch-government-websites/#disqus_thread

DutchNews.nl. (2015b). The Netherlands is popular with cyber criminals. Retrieved August 20, 2015, from http://www.dutchnews.nl/news/archives/2015/04/the-netherlands-is-popular-with-cyber-criminals/

Dutta, A., & Mccrohan, K. (2002). Management's role in Information Security in a Cyber Economy. *California Management Review*, (Fall), 67–87.

Ebrahim, Z., & Irani, Z. (2005). E-government adoption: architecture and barriers. *Business Process Management Journal*, *11*(5), 589–611. doi:10.1108/14637150510619902

EPractice. (2012). NL: Dutch Customs - Millions of messages processed quickly and efficiently via Digipoort. Retrieved August 20, 2015, from https://joinup.ec.europa.eu/community/epractice/news/nl-dutch-customs-millions-messages-processed-quickly-and-efficiently-digipo

European Commission. (2010). *The European eGovernment Action Plan 2011-2015 Harnessing ICT to promote smart, sustainable & innovative Government*. Brussels. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF

Fang, Z. (2002). E-government in digital era: concept, practice, and development. *International Journal of the Computer, the Internet and …*, *10*(2), 1–22. Retrieved from http://sahra.org.za/sites/default/files/additionaldocs/10.1.1.133.9080.pdf

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, *6*(2-3), 203–225.

Fehr, S. (2011). Information Theoretic Security. In S. Fehr (Ed.), *5th International Conference, ICITS, Amsterdam*. Amsterdam: Springer Heidelberg Dordrecht London New York. doi:10.1007/978-3-642-20728-0

Fisher, W. W., Tinsley, D., & Strader, R. (2009). Managing Unavoidable Risks in Cloud Computing. *Journal of Business Issues*, (1), 1–11. Retrieved from http://uwf.edu/media/university-of-west-florida/colleges/cob/deans-office-pdfs/journal-of-business-issues/JBI2009-1.pdf#page=5

Fox IT. (2015). RSA-512 Certificates abused in the wild. Retrieved August 2, 2015, from http://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/

Frates, C., & Devine, C. (2014). Government hacks and security breaches skyrocket. Retrieved January 30, 2015, from http://edition.cnn.com/2014/12/19/politics/government-hacks-and-security-breaches-skyrocket/

Furnell, S. (2005). Why users cannot use security. *Computers & Security*, *24*(4), 274–279. doi:10.1016/j.cose.2005.04.003

Graux, H., & Majava, J. (2007). *eID Interoperability for PEGS - Analysis and Assessment of similarities and differences - Impact on eID interoperability*. Retrieved from http://ec.europa.eu/idabc/servlets/Doc0939.pdf?id=29618

Halchin, L. E. (2004). Electronic government: Government capability and terrorist resource. *Government Information Quarterly*, *21*(4), 406–419. doi:10.1016/j.giq.2004.08.002

Hanna, N. K., & Qiang, C. Z. (2009). *National E-Government Institutions: Functions, Models, and Trends*. *Information and Communications for Development 2009*. Washington DC: World Bank Group. doi:10.1596/978-0-8213-7605-8

Henriksen, H. Z., Rukanova, B., & Tan, Y. H. (2008). Pacta Sunt Servanda but where is the agreement? The complicated case of eCustoms. *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5184 LNCS*, 13–24. doi:10.1007/978-3-540-85204-9_2

Highteck.net. (2015). Application Layer ISO OSI Functionality and Protocols. Retrieved April 20, 2015, from http://www.highteck.net/EN/Application/Application_Layer_Functionality_and_Protocols.html

Holtfreter, K. (2005). Is occupational fraud "typical" white-collar crime? A comparison of individual and organizational characteristics. *Journal of Criminal Justice*, *33*(4), 353–365. doi:10.1016/j.jcrimjus.2005.04.005

Hong, C. R., Randall, Choy, N., Tiep, D. V., & Mcintyre, D. (2012). An assessment on public key infrastructure's security concerns. In *CS2107 - Semester IV, 2012* (Vol. 2107, pp. 48–53). Singapore.

Hoogstraaten, H., Prins, R., Niggebrugge, D., Heppener, D., Groenewegen, F., Wettinck, J., … Hu, Y. Z. (2012). *Black Tulip: Report of the investigation into the DigiNotar Certificate Authority breach*. Netherlands.

Houlding, D., Casey, T., & Rosenquist, M. (2012). *Improving Healthcare Risk Assessments to Maximize Security Budgets*. *Healthcare Information Security*.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255. doi:10.1016/j.istr.2008.10.010

Hunt, R. (2001a). PKI and digital certification infrastructure. *IEEE International Conference on Networks, ICON*, 234–239. doi:10.1109/ICON.2001.962346

Hunt, R. (2001b). Technological infrastructure for PKI and digital certification. *Computer Communications*, *24*(14), 1460–1471. doi:10.1016/S0140-3664(01)00293-6

Jacobi, A., Jensen, M. L., Kool, L., Munnichs, G., & Weber, A. (2013). Security of eGovernment Systems. In *Science and Technology Options Assessment* (pp. 1–80). Brussels. doi:10.2861/29262

Joshi, J., Ghafoor, A., Aref, W. G., & Spafford, E. H. (2001). Digital government security infrastructure design challenges. *Computer*, *34*(2), 66–72. doi:10.1109/2.901169

Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, *32*, 489–496. doi:10.1016/j.procs.2014.05.452

Kefallinos, D., Lambrou, M. A., & Sykas, E. D. (2006). A Secure PKI enabled NAtional e-government infrastructure: SYZEFXIS Case. In D. Remenyi (Ed.), *Proceedings of the 6th European Conference on e-Government*. Reading: Academic Conferences Limited.

KPMG. (2011). *Who is the typical fraudster ?* Retrieved from https://www.kpmg.com/CEE/en/IssuesAndInsights/ArticlesPublications/Documents/who-is-the-typical-fraudster.pdf

Lacity, M. C., & Hirschheim, R. (1993). The Information Systems Outsourcing Bandwagon. Retrieved April 27, 2015, from http://sloanreview.mit.edu/article/the-information-systems-outsourcing-bandwagon/

Lamsweerde, a. Van. (2000). Requirements engineering in the year 00: a research perspective. *Proceedings of the 2000 International Conference on Software Engineering. ICSE 2000 the New Millennium*, 5–19. doi:10.1109/ICSE.2000.870392

Laudon, K., & Jane, L. (2012). *Management Information Systems* (12th ed.). New Jersey: Prentice Hall.

Lindqvist, U., & Jonsson, E. (1997). How to systematically classify computer security intrusions. In *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)* (pp. 154–163). IEEE Comput. Soc. Press. doi:10.1109/SECPRI.1997.601330

Logius. (2015a). Certifications. Retrieved August 2, 2015, from http://www.sbr-nl.nl/actueel/veelgestelde-vragen/certificaten

Logius. (2015b). CSP certificates. Retrieved August 2, 2015, from https://www.logius.nl/standaarden/pkioverheid/certificaten/csp-certificaten/

Logius. (2015c). Customs Declarations. Retrieved April 20, 2015, from https://www.logius.nl/ondersteuning/gegevensuitwisseling/douane-import-export-expeditie/

Logius. (2015d). Data Delivery DNB. Retrieved April 20, 2015, from https://www.logius.nl/ondersteuning/gegevensuitwisseling/de-nederlandsche-bank/

Logius. (2015e). Data Delivery EBV Tax. Retrieved April 20, 2015, from https://www.logius.nl/ondersteuning/gegevensuitwisseling/belastingdienst-ebv-banken-verzekeraars/

Logius. (2015f). Data exchange. Retrieved April 20, 2015, from https://www.logius.nl/over-logius/jaaroverzichten/jaaroverzicht-2012/producten/gegevensuitwisseling/

Logius. (2015g). Declarations NVWA. Retrieved April 20, 2015, from https://www.logius.nl/ondersteuning/gegevensuitwisseling/nvwa-visvaartuigen-importeurs/

Logius. (2015h). Digikoppeling. Retrieved June 28, 2015, from https://www.logius.nl/diensten/digikoppeling/

Logius. (2015i). Digipoort. Retrieved April 20, 2015, from https://www.logius.nl/over-logius/jaaroverzichten/jaaroverzicht-2012/producten/gegevensuitwisseling/digipoort/

Logius. (2015j). EU Tax and VAT returns. Retrieved April 20, 2015, from https://www.logius.nl/ondersteuning/gegevensuitwisseling/belastingdienst-eu-btw-retour/

Logius. (2015k). Koppelvlak WUS 2.0 voor bedrijven. Retrieved June 28, 2015, from https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-bedrijven/

Logius. (2015l). PKIoverheid. Retrieved April 20, 2015, from https://www.logius.nl/over-logius/jaaroverzichten/jaaroverzicht-2012/producten/toegang/pkioverheid/

Logius. (2015m). PKIoverheid. Retrieved April 22, 2015, from https://www.logius.nl/languages/english/pkioverheid/

Logius. (2015n). Program of Requirements. Retrieved April 22, 2015, from https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-csp/programma-van-eisen/

Logius. (2015o). Purchase certificates. Retrieved April 22, 2015, from https://www.logius.nl/diensten/pkioverheid/aanschaffen/

Logius. (2015p). Services Digipoort. Retrieved April 20, 2015, from https://www.logius.nl/over-logius/jaaroverzichten/jaaroverzicht-2012/producten/gegevensuitwisseling/

Logius. (2015q). SETU (HR-XML) - OHNL. Retrieved July 4, 2015, from https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl/

Logius. (2015r). Standard business reporting. Retrieved July 15, 2015, from http://www.sbr-nl.nl/

Logius. (2015s). UBL-OHNL. Retrieved July 4, 2015, from https://www.logius.nl/ondersteuning/gegevensuitwisseling/e-factureren-voor-leveranciers/

Lucas, E. (2015, February). Why we are not ready for cyberwar. *The Security Times*, (February), 33. Retrieved from https://www.securityconference.de/fileadmin/MSC_/PDF/Security_Times_2009-2013/Security_Times_Feb2015.pdf

Marinos, L. (2013). *ENISA Threat Landscape 2013 Overview of current and emerging cyber-threats*. doi:10.2788/14231

Marinos, L. (2014). *ENISA Threat Landscape 2014*. ENISA. doi:10.2824/061861

Marinos, L., & Sfakianakis, A. (2012). ENISA Threat Landscape - Responding to the Evolving Threat Environment, 96. Retrieved from http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). Cyber Threat Metrics. *Sandia National Laboratories*, (March). doi:10.2172/1039394

Meulen, N. Van Der. (2013). DigiNotar : Dissecting the First Dutch Digital Disaster. *Journal of Strategic Security*, *6*(2), 46–58. Retrieved from http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1246&context=jss

MITRE. (2014). Cyber Threat Susceptibility Assessment. Retrieved from http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/cyber-threat-susceptibility-assessment

Möckel, C., & Abdallah, A. E. (2010). Threat modeling approaches and tools for securing architectural designs of an e-banking application. *2010 6th International Conference on Information Assurance and Security, IAS 2010*, 149–154. doi:10.1109/ISIAS.2010.5604049

Moon, M. J. (2002). The Evolution of E-Government among Municipalities: Rhetoric or Reality? *Public Administration Review*, *62*, 424–433. doi:10.1111/0033-3352.00196

Murphy, P. R., & Dacin, M. T. (2011). Psychological Pathways to Fraud: Understanding and Preventing Fraud in Organizations. *Journal of Business Ethics*, *101*(4), 601–618. doi:10.1007/s10551-011-0741-0

Myagmar, S., Lee, A., & William, Y. (2005). Threat Modeling as a Basis for Security Requirements. *In StorageSS '05: Proceedings of the 2005 ACM Workshop on Storage Security and Survivability*, 94–102.

NCSC. (2014). *Cyber Security Assessment Netherlands*. Den Haag. Retrieved from https://english.nctv.nl/publications-products/Cyber_Security_Assessment_Netherlands/

Network World. (2010). RSA 1024-bit private key encryption cracked. Retrieved August 2, 2015, from http://www.techworld.com/news/security/rsa-1024-bit-private-key-encryption-cracked-3214360/

Networking4all. (2011). Time-line for the DigiNotar hack. Retrieved June 30, 2015, from https://www.networking4all.com/en/ssl+certificates/ssl+news/time-line+for+the+diginotar+hack/

Networking4all. (2015). CSR Decoding / CSR Verification. Retrieved August 8, 2015, from http://www.networking4all.com/en/support/tools/csr+check/

OECD. (2008). Future of e-government AGENDA 2020. In *OECD E-Leaders Conference 2008*. The Hague: OECD. Retrieved from www.oecd.org/dataoecd/41/40/43340370.pdf

Palvia, S. C. J., & Sharma, S. S. (2007). E-Government and E-Governance : Definitions / Domain Framework and Status around the World. In *5th International Conference on E-governance (ICEG)* (pp. 1–12). Computer Society of India. Retrieved from http://www.csi-sigegov.org/1/1_369.pdf

Posey, B. (2005). A beginner's guide to Public Key Infrastructure. Retrieved April 22, 2015, from http://www.techrepublic.com/article/a-beginners-guide-to-public-key-infrastructure/

Prins, J. . (2011). *Interim Report - DigiNotar Certificate Authority breach "Operation Black Tulip."*

Privacy Rights Clearinghouse. (2015). Chronology of Data Breaches | Privacy Rights Clearinghouse. Retrieved February 8, 2015, from https://www.privacyrights.org/data-breach/

Riad, a. M., El-Bakry, H. M., & El-Adl, G. H. (2011). E-government Frameworks Survey. *International Journal of Computer Science Issues (IJCSI)*, *8*(3), 319–323. doi:Article

Rosenquist, M. (2009). *Whitepaper: Prioritizing Information Security Risks with Threat Agent Risk Assessment*. *USA: Intel Information Technology*. Retrieved from https://communities.intel.com/community/itpeernetwork/blog/2010/01/05/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment

Ruf, L., Ag, C., Thorn, A., Gmbh, A., Christen, T., Financial, Z., … Luzern, H. (2003). Threat Modeling in Security Architecture – The Nature of Threats Threat Model. *Information Security Society Switzerland*, (June), 1–4.

Scahill, J., & Begley, J. (2015). The great sim heist. Retrieved August 8, 2015, from https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

Sein, M. K., Henfridsson, O., Rossi, M., & Lindgren, R. (2011). Action Design Research. *MIS Quarterly*, *35*(1), 37–56.

Shostack, A. (2014). *Threat Modeling*. (C. Long, Ed.). BoulevardIndianapolis: John Wiley & Sons, Inc.

Spetalnick, M., & Brunnstrom, D. (2015). China in focus as cyber attack hits millions of U.S. federal workers. Retrieved July 20, 2015, from http://www.reuters.com/article/2015/06/05/us-cybersecurity-usa-idUSKBN0OK2IK20150605

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. doi:10.1016/j.cose.2004.07.001

Stiennon, R. (2010). Seven Cyber Scenarios To Keep You Awake At Night. Retrieved January 24, 2015, from http://www.forbes.com/sites/firewall/2010/04/29/seven-cyber-scenarios-to-keep-you-awake-at-night/2/

Symantec. (2014). The Threat Landscape in 2014 and Beyond: Symantec and Norton Predictions for 2015, Asia Pacific & Japan. Retrieved August 22, 2015, from http://www.symantec.com/connect/blogs/threat-landscape-2014-and-beyond-symantec-and-norton-predictions-2015-asia-pacific-japan

Symantec Corporation. (2014). Internet Security Threat Report, *19*(April), 97. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Telang, R., & Wattal, S. (2005). Impact of Software Vulnerability Announcements on the Market Value of Software Vendors – An Empirical Investigation. In *Fourth Workshop on the Economics of Information Security (WEIS)*. Cambridge, MA. Retrieved from http://opim.wharton.upenn.edu/wise2004/sat622.pdf

The Economist. (2000). Handle with care. Retrieved from http://www.economist.com/node/80866

The Open Group. (2009). *Risk Taxonomy*. Retrieved from http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf

The Open Group. (2010). *Technical Guide FAIR – ISO / IEC 27005 Cookbook*. Retrieved from http://www.businessofsecurity.com/docs/FAIR - ISO_IEC_27005 Cookbook.pdf

Tropina, T. (2015). Cyber Crime and Organized Crime. Retrieved May 21, 2015, from http://f3magazine.unicri.it/?p=310

UN. (2011). Cybersecurity: A global issue demanding a global approach. Retrieved May 7, 2015, from http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

UN. (2014). UN E-Government Survey 2014. Retrieved August 20, 2015, from http://unpan3.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014

Verizon. (2015a). 2013 Industry Threat Landscape Reports. Retrieved August 22, 2015, from http://www.verizonenterprise.com/DBIR/2013/industries/

Verizon. (2015b). veriscommunity. Retrieved May 7, 2015, from http://veriscommunity.net/index.html

Vidalis, S., Jones, A., & Blyth, A. (2004). Assessing cyber-threats in the information environment. *Network Security*, *2004*(November), 10–16. doi:10.1016/S1353-4858(04)00156-4

Vieira, P., & King, C. (2014). Canadian Government Reports Cyberattack. Retrieved July 20, 2015, from http://www.wsj.com/articles/canadian-government-reports-cyberattack-1406638057

W3C. (2004). *Web Services Architecture*. *W3C Working Group Note*. Retrieved from http://www.w3.org/TR/ws-arch/wsa.pdf

Wagstyl, S. (2015). Ukraine separatists claim cyber attack on German government sites. Retrieved January 24, 2015, from http://www.ft.com/cms/s/0/08270324-9678-11e4-a40b-00144feabdc0.html#axzz3PmBJMEzG

Wijk, R. van. (2015). De keten uitgedaagd. Retrieved August 2, 2015, from http://www.sbr-nl.nl/fileadmin/SBR/documenten/Communicatie/SBR_College9_RvW.pdf

Yang, B., Li, Q., & Zuo, M. (2008). Analysis of E-Government Outsourcing. In L. D. Xu, A. M. Tjoa, & S. S. Chaudhry (Eds.), *Research and Practical Issues of Enterprise Information Systems II* (Vol. 2, pp. 1191–1195). Boston, MA: Springer US. doi:10.1007/978-0-387-76312-5

Zalewski, J., Drager, S., McKeever, W., & Kornecki, A. J. (2013). Threat modeling for security assessment in cyberphysical systems. *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop on - CSIIRW '13*, 1. doi:10.1145/2459976.2459987

Zeltser, L. (2015). How Digital Certificates Are Used and Misused. Retrieved June 20, 2015, from https://zeltser.com/how-digital-certificates-are-used-and-misused/

Appendices

Appendix I

E-mail Services and Protocols

E-mail revolutionized how people communicate through its simplicity and speed. Email requires several applications and services to function. Figure 26 shows two of the Application layer protocols used by emails - Post Office Protocol (POP), the latest being POP3 and Simple Mail Transfer Protocol (SMTP). Similar to HTTP, these protocols define client/server processes. When we compose e-mail messages, we typically use an application called a Mail User Agent (MUA), or e-mail client. The MUA enables us to send messages and places received messages into our mailbox, both of which are distinct processes. In order to receive e-mail messages from an e-mail server, the e-mail client can use POP3. Sending e-mail from either a client or a server uses message formats and command strings defined by the SMTP protocol. Usually an e-mail client provides the functionality of both protocols within one application (Highteck.net, 2015).

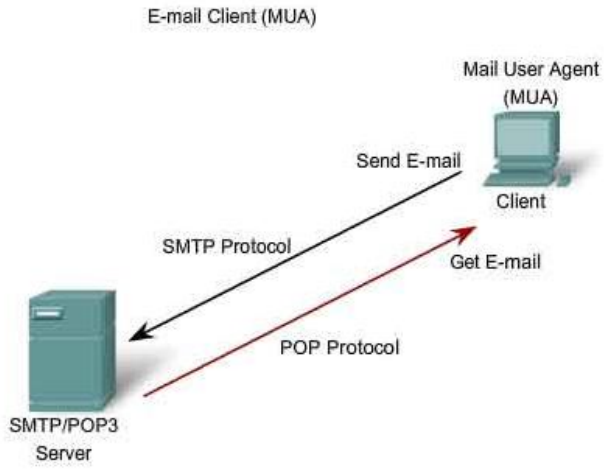

Figure 26: Email protocols, adopted from (Highteck.net, 2015)

E-mail Server Processes - MTA and MDA

The e-mail server operates two separate processes:

- *Mail Transfer Agent (MTA)*
  The MTA process is used to forward e-mail. As shown in the Figure 27, the MTA receives messages from the MUA or from another MTA on another e-mail server. Based on the message header, it determines how a message has to be forwarded to reach its destination.
- *Mail Delivery Agent (MDA)*
  When the mail is addressed to a user whose mailbox is on the local server, the mail is passed to the MDA. If the user is not part of the local server, then MTA routes the e-mail to the MTA on the appropriate server. In Figure 27, we see that the Mail Delivery Agent (MDA) accepts a piece of e-mail from a Mail Transfer Agent (MTA) and performs the actual delivery. The MDA receives all the inbound mail from the MTA and places it into the appropriate users' mailboxes.

Most e-mail communications use the MUA, MTA, and MDA applications. However, a client may be connected to a corporate e-mail system, such as IBM's Lotus Notes, Novell's Groupwise, or Microsoft's Exchange. These systems often have their own internal e-mail format, and their clients typically communicate with the e-mail server using a proprietary protocol. As another alternative, computers that do not have an MUA can still connect to a mail service on a web browser in order to retrieve and send messages in this manner.

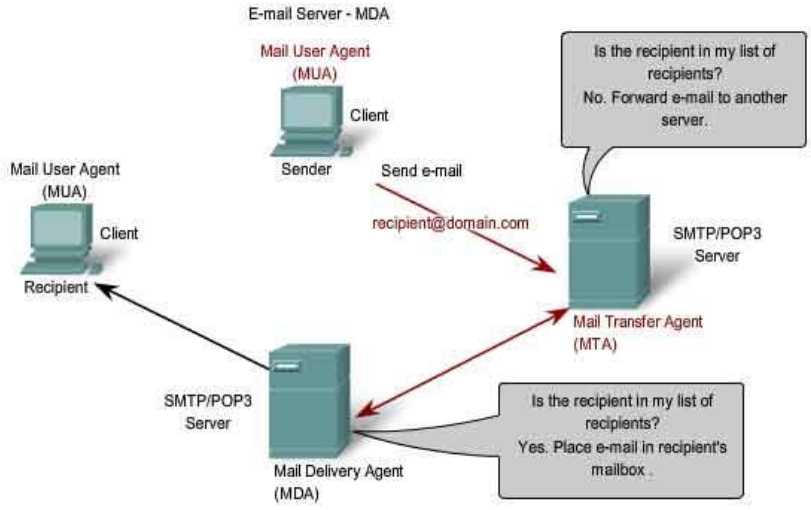

Figure 27: Email communications, adopted from (Highteck.net, 2015)

POP and SMTP

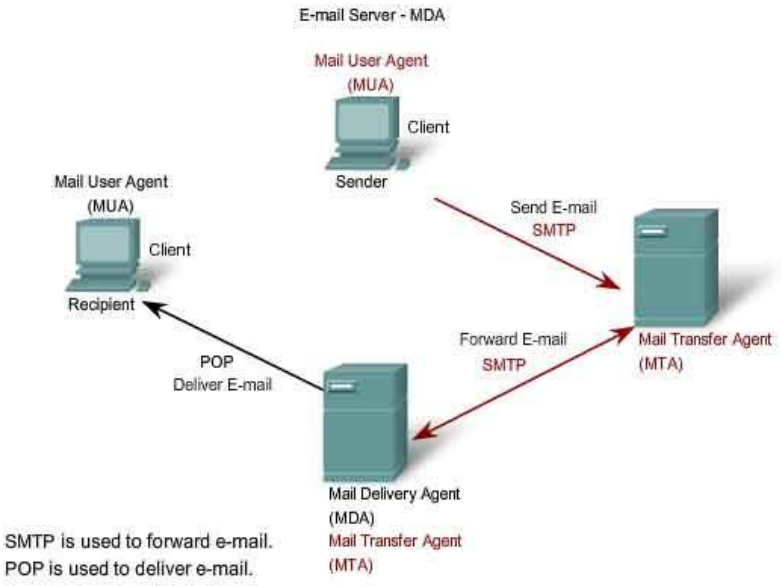

Figure 28: Functions of SMTP & POP protocols, adopted from (Highteck.net, 2015)

POP and POP3 (Post Office Protocol, version 3) are inbound mail delivery protocols and are typical client/server protocols. They deliver e-mail from the e-mail server to the client (MUA). The MDA waits for a client to connect to a server. When a connection is established, the server will deliver the e-mail to the client. The SMTP however, governs the transfer of outbound e-mail from the sending client to the e-mail server (MDA), as well as the transport of e-mail between e-mail servers (MTA). SMTP allows e-mails to be transported across networks between different types of client software and servers and makes e-mail exchange over the Internet possible (Highteck.net, 2015). Figure 28 shows the functions of SMTP and POP protocols.

FTP

The File Transfer Protocol (FTP) is another commonly used Application layer protocol. FTP enables file transfers between a client and a server. An FTP client application runs on a computer and is used to push and pull files from a server running the FTP daemon (FTPd). To successfully transfer files, FTP requires two connections between the client and the server: one for commands and replies, the other for the actual file transfer. The file transfer can happen in either direction. The client can download (pull) a file from the server or, the client can upload (push) a file to the server (Highteck.net, 2015).

Comparison of Digipoort OTP and Digipoort PI

Table 24: Comparison of Digipoort OTP and PI

	Digipoort OTP	Digipoort PI
Purpose	Electronic message transfer	Electronic message transfer
Interfaces used by businesses	SMTP, FTP and POP3	WUS
Interfaces used by governments	X.400, SMTP, FTP and POP3	Digikoppelling WUS, Digikoppelling ebMS
Uses web service	No	Yes
Uses PKI	Yes	Yes
Uses XML, XBRL	No	Yes
Government agencies using the service	Douane, Belastingdienst, NVWA, DNB etc	Belastingdienst, Chamber of Commerce, Central Bureau of Statistics
Message structure	Email	SOAP

Appendix II

Extract of Past Incidents in the Public Sector

Sl. No	Date	Affected Organization	Description	Agent	Assets Compromised	Objective			Method						Reference
						Motivation	Goal	Objective	Acts					Limits	
									Copy, expose	Deny, Withhold, Ransom	Destroy, Delete, Render unavailable	Damage, Alter	Take, Remove		
1	14-Apr-15	Damariscotta County Sheriff's Department Damariscotta, Maine	Malware installation by clicking a link, and withholding confidential information.	Mobster	Information	Personal financial gain & Organizational gain	Deny access, ask ransom	Theft/Exposure, Data Loss, Sabotage, Operations Impact		x	x	x	x	Extra-legal, major	http://www.eteknix.com/us-police-forced-to-pay-bitcoin-ransom/
2	13-apr-15	Grapevine Police Departments Grapevine, Texas	Database hacked and a video was posted.	Civil Activist	Database	Ideology	Change public opinion or corporate policy	Sabotage, Embarrassment				x		Extra-legal, minor	http://thescoopblog.dallasnews.com/2015/04/anonymous-hacker-group-demands-police-video-of-shooting-of-mexican-immigrant-by-grapevine-cop.html/
3	25-nov-14	Texas Health and Human Services Houston, Texas	End of contract dispute with Xerox regarding the ownership of assets containing data.	Vendor (Intentional)	Documents and data	Organizational gain	Deny access	Data loss		x			x	Legal	http://www.govinfosecurity.com/breach-reported-after-vendor-dispute-a-7605
4	25-nov-14	State Compensation Insurance Fund Pleasanton,	Data breach when one of their brokers suffered a data breach to their	Vendor Reckless/Vendor error	Data	Accidental	No malicious intent	Theft/Exposure, Data loss	x					Legal	http://oag.ca.gov/system/files/11242014%20Notification%20Letter_AFF

		California	system.												ECTED_PROOF_0.pdf?
5	17-nov-14	US State Department Washington, District Of Columbia	The US State Department said Monday it shut down its unclassified computer network over the weekend after evidence emerged that it could have been hacked. The Washington Post quoted sources as saying hackers believed to be working for the Russian government were believed to be responsible for that breach.	Foreign Governme nt Spy	System handling non-classified emails	Political Loyalty/ Ideology	Access confidenti al data	Theft/Exposure	x				x	Extra-legal, major	http://phys.org/news/2014-11-state-dept-hacked-email.html#inlRlv
6	10-nov-14	US Postal Service Washington, District Of Columbia	Chinese hackers attacked computer networks compromising the information of over 800,000 employees.	Foreign Governme nt Spy	Networks, Database, Information	Political Loyalty/ Ideology	Access confidenti al data	Theft/Exposure	x					Extra-legal, major	http://www.washingtonpost.com/blogs/federal-eye/wp/2014/11/10/china-suspected-of-breaching-u-s-postal-service-computer-networks/
7	10-Oct-14	Department of Human Services' Office of Behavioral Health, Denver	Data breach when a postcard mailing went out with confidential information to individuals as part of a survey.	Employee s Error	Information	Accidental	No malicious intent	Theft/Exposure	x					Code-of-Conduct	http://www.9news.com/story/news/local/2014/10/10/colorado-health-officials-announce-privacy-breach/17055779/
8	12-Sep-14	Health and Human Services Agency, Napa Napa, California	Data breach when one of their flash/thumb drives was missing from their offices.	Thief	USB containing information	Personal financial gain	Steal PII	Theft/Exposure	x				x	Extra-legal, minor	http://oag.ca.gov/system/files/Redacted%20copy%20of%20standerd%20IHSS%20notification%20letter%20sent%20to%20all%20affected%20IHSS%20clients_0.pdf?

9	22-May-14	Alabama Department of Public Health Montgomery, Alabama	Employee using inside information to perform tax fraud.	Internal spy	Personal/tax information	Personal financial gain	Steal PII	Theft/Exposure	x					Extra-legal, minor	http://data-breach.silk.co/page/Department-of-Public-Health-Alabama-22-05-2014
10	3-Mar-14	City of Detroit Detroit, Michigan	The City of Detroit announced a security breach that affected files of approximately 1,700 city employees. Apparently the breach occurred when an employee clicked on a software link that contained malicious software that released a code that froze access to numerous files.	Employee Reckless	Information	Accidental	No malicious intent	Theft/Exposure, Data Loss, Operations Impact	x		x	x		Legal	http://www.myfoxdetroit.com/story/24867915/detroit-reports-recent-computer-security-breach
11	17-Dec-13	Colorado Governor's Office of Information Technology Denver, Colorado	A Colorado state employee lost a flash drive that contained the information of current and former Colorado state employees. It contained names, Social Security numbers, and a limited number of home addresses. Employee did not follow protocol.	Employee Reckless	Information	Accidental	No malicious intent	Theft/Exposure	x		x	x		Legal	http://www.denverpost.com/news/ci_24734928/sensitive-data-lost-19-000-colorado-employees
12	16-Dec-13	Tennessee Department of Treasury Nashville, Tennessee	An employee downloaded the information of 6,300 Nashville teachers in order to work from a personal computer and account at home. Police later charged him with theft of data, considering his suspicious web searches about selling social security numbers.	Internal spy	Information downloaded	Personal financial gain	Take	Theft/Exposure	x					Extra-legal, minor	http://www.databreaches.net/tn-former-state-treasury-employee-charged-with-identity-theft-trafficking/
13	2-Dec-13	Board of	Office burglary of a	Thief	Information loss	Personal	Take	Theft/Exposure	x				x	Extra-	http://www.efort

		Barbering and Cosmetology Sacramento, California	desktop computer resulted in the exposure of sensitive information.		due to theft of desktop computer	financial gain								legal, minor	resses.com/2013-Breaches-Matrix.htm
14	11-Nov-13	New York City Police Department New York, New York	A former police detective payed hacker to steal passwords associated with the email accounts of other officers. The detective also misused the National Crime Information Center database to search for the information of at least two other NYPD officers.	Employee Disgruntled	Information	Disgruntlement	Damage or retributio n	Sabotage, Embarrassment	x					Extra-legal, minor	https://www.fbi.gov/newyork/press-releases/2013/nypd-detective-pleads-guilty-in-manhattan-federal-court-to-computer-hacking
15	8-Nov-13	Baltimore County Baltimore, Maryland	A contractor who worked for Baltimore County was found to have saved the personal information of 12,000 county employees to computers for reasons unrelated to work.	Vendor (Intentional)	Information downloaded	Organizational gain	Theft	Theft/Exposure	x				x	Legal	http://www.bizjournals.com/baltimore/blog/cyberbizblog/2013/11/baltimore-county-reports-additional.html
16	6-Sep-13	Georgia Department of Labor Marrieta, Georgia	An employee accidentally emailed a document with the names and Social Security numbers of Cobb-Cherokee Career Center customers to 1,000 people.	Employee Error	Information disclosure	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://www.11alive.com/news/article/305333/40/Email-with-thousands-of-SSNs-sent-to-Dept-of-Labor-customers
17	5-Sep-13	North Texas Comprehensive Spine and Pain Center Sherman, Texas	A former employee stole an external hard drive that contained the medical information of patients. There has been no evidence that the information on the hard drive was improperly used.	Thief	Stolen hard drive	Personal financial gain	Take	Theft/Exposure					x	Extra-legal, minor	http://www.scmagazine.com/employee-fired-for-stealing-external-hard-drive-containing-patient-data/article/308109/
18	23-Aug-13	Hill Air Force Base Ogden, Utah	An administrative employee sent the names and Social	Employee Reckless	Information	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://www.standard.net/stories/2013/08/23/hill-

			Security numbers of Hill Air Force Base employees to a personal email account. The administrative employee planned to finish a project at home but transferring the information to an unprotected email address may have resulted in the exposure of information. The employee's actions were against Hill Air Force Base policy.													employee-personal-info-improperly-transmitted
19	3-Jul-13	Indiana Family and Social Services Administration (FSSA), RCR Technology Corporation Indianapolis, Indiana	A computer programming glitch resulted in the exposure of client health, financial, and employment information. Personal and private documents that belonged to certain clients were accidentally made available to other clients between April 6 and May 21 when FSSA contractor RCR Technology Corporation made a programming error.	Vendor Reckless/Vendor error	Information	Accidental	No malicious intent	Theft/Exposure, Data loss	X					Legal	http://www.in.gov/activecalendar/EventList.aspx?fromdate=7/1/2013&todate=7/1/2013&display=Month&type=public&eventidn=109586&view=EventDetails&information_id=183960&print=print
20	6-Jun-13	Town of Brookhaven Brookhaven, New York	A law enforcement employee made a clerical error that caused the Social Security numbers of 78 ambulance workers and beneficiaries to be available on the town website for five days.	Employee Error	Information disclosure	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://www.newsday.com/long-island/towns/brookhaven-data-breach-was-clerical-error-officials-say-1.5426405
21	16-May-	City of Akron	Cyber hackers from	Civil	websites, data	Ideology	Change	Theft/Exposure,	x	x	x	x		Extra-	http://www.data

	13	Akron, Ohio	Turkey hacked into the city of Akron's website and replaced city messages with politically-motivated ones on Thursday. Also, nearly 8,000 taxpayers had their personal information stolen including their names, addresses, and social security numbers.	activist			public opinion or corporate policy	Sabotage, Operations impact, Embarrassment						legal, minor	breaches.net/fbi-city-of-akron-investigating-hacker-attack-that-compromised-identities-of-8000-taxpayers/
22	8-May-13	Department of Family and Support Services (DFSS) Chicago, Illinois	Computer equipment was reported stolen from the Department of Family Support Services. The types of information that may have been on the device or devices were not reported.	Thief	Information loss due to burglary of computer equipment	Personal financial gain	Take	Theft/Exposure	x				x	Extra-legal, minor	http://healthitsecurity.com/news/theft-at-dfss-in-chicago-could-lead-to-health-data-breach
23	31-Mar-13	Allen County Lima, Ohio	An administrative error caused the Social Security numbers and other personal information of Allen County employees to be available online for less than an hour.	Employee Error	Information disclosure	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://www.nfvzone.com/news/2013/03/31/7028026.htm
24	28-Mar-13	Tooele County Tooele, Utah	A former employee received a CD with the names and Social Security numbers of around 200 current and former employees when he requested his personnel file. When the HR department realized their mistake they requested that the former employee return the CD. He gave the CD to the Tooele County Attorney's office.	Employee Reckless	Information disclosure	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://www.sltrib.com/sltrib/news/56068416-78/brozovich-county-information-tooele.html.csp
25	22-Feb-13	Minnesota Department of	An employee working as an administrative	Employee Reckless	Information disclosure	Accidental	No malicious	Theft/Exposure	x					Legal	http://www.twincities.com/ci_2245

		Natural Resources, Minnesota Department of Motor Vehicles Little Falls, Minnesota	manager in the Enforcement Division viewed the DMV information of around 5,000 people outside of work hours and for no job-related reason. It is believed that the driver's license and other motor vehicle record information were viewed for curiosity and not malicious purposes.				intent								1214/minnesota-dnr-identifies-ex-worker-who-accessed-data
26	8-Feb-13	United States Federal Reserve, Grand Banks Yachts Washington, District Of Columbia	The hacking group known as Anonymous claimed responsibility for a hack of the Alabama Criminal Justice Center and indicated that they had access to US Federal Reserve servers. Some internal documents were also exposed. The hack attack was a response to the US Federal Reserve's reaction, or failure to react, to the February 4 hack of the Alabama Criminal Justice Center.	Civil activist	Servers, internal documents	Ideology	Change public opinion or corporate policy	Theft/Exposure, embarrassment			x	x		Extra-legal, minor	https://www.privacyrights.org/node/56005
27	28-Jan-13	Los Angeles County Department of Public Social Services Los Angeles, California	A former employee with the Los Angeles County Department of Public Social Services ("DPSS") pleaded guilty today to a single identity theft violation and admitted that identities she stole from the county were used to file fraudulent tax returns in the names of 64 different people causing a loss to the Internal Revenue Service of over $357,000. The	Internal spy	Information theft	Personal financial gain	Steal information	Theft/Exposure	x					Extra-legal, minor	http://www.irs.gov/uac/Former-Los-Angeles-County-Employee-Pleads-Guilty-to-Identity-Theft-Scam

			employee, her spouse, and three others were indicted in January of 2012.													
28	13-Nov-12	Chicago Board of Elections Commissioners Chicago, Illinois	The sensitive information of Chicago voters was exposed online due to a mistake by the election authority. A database that included names, the last four digits of Social Security numbers, addresses, and drivers license numbers was accidentally placed online in a publicly accessible place.	Employee Error	Information	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://www.databreaches.net/chicago-election-site-exposed-personal-information/
29	19-Oct-12	U.S. National Weather Service, Weather.gov Silver Spring, Maryland	Hackers targeted the U.S. National Weather Service website Weather.gov in an attempt to exploit vulnerabilities in U.S. government online systems. The hackers claim to have begun a campaign in response to U.S. cyberattacks in Muslim nations.	Civil activist	Login credentials, system and network configuration files	Ideology	Change public opinion or corporate policy	Operations impact, embarrassment	x	x	x	x		Extra-legal, minor	https://www.novainfosec.com/2012/10/21/rfi-leads-to-hacked-weather-site/
30	12-Oct-12	Army Material Command Huntsville, Alabama	An employee transported a hard copy of sensitive employee documents home. The employee is not believed to have taken the information for fraudulent or criminal activity.	Employee reckless	Information	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://blog.al.com/breaking/2012/10/army_materiel_command_on_redst.html
31	2-Oct-12	Town Council of Chapel HillChapel Hill, North Carolina	A licensed clinical social worker accidentally attached confidential client information to anemail that was forwarded to town council colleagues. A copy of her and her	Employee Error	Information	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://www.privatewifi.com/data-breaches-continue-to-happen-at-banks-colleges-and-beyond/

			husband's 2011 income tax returns was also in the email. The email automatically became available to the publicand the error was noticed nearly a week later. The information was publicly available for aweek.													
32	28-Sep-12	Brightline Interactive, Army Chief of Public Affairs Alexandria, Virginia	An army awards database was found to be available online. The database was being handled by the defense contractor Brightline Interactive and was mistakenly uploaded to a public server at an unknown time. Those who received awards for actions since September 11, 2001 were affected.	Vendor reckless/Vendor error	Database	Accidental	No malicious intent	Theft/Exposure, Data loss	x					Legal	http://archive.armytimes.com/article/20120928/NEWS/209280324/MoH-DSC-recipients-Social-Security-numbers-exposed
33	23-Sep-12	Town of Willimantic, Connecticut Willimantic, Connecticut	An employee's laptop was stolen from his unattended office. The laptop was password-protected. It contained the information of town employees. Social Security and bank account numbers may have been exposed.	Thief	Information loss due to burglary of computer equipment	Personal financial gain	Take	Theft/Exposure	x				x	Extra-legal, minor	http://www.norwichbulletin.com/article/20120924/News/309249943
34	6-Sep-12	Boston Water and Sewer Commission Boston, Massachusetts	A contractor working for Boston Water and Sewer Commission misplaced a hard drive. The hard drive may have contained customer names, account numbers, meter numbers, phone numbers, addresses, and other	Vendor reckless	Hard drive, information	Accidental	No malicious intent	Theft/Exposure, Data loss	x		x	x	x	Legal	http://www.alertboot.com/blogs/endpoint_security/archive/2012/09/07/data-breach-boston-water-and-sewer-commission-contractor-loses-hard-drive.aspx

			information the utility organization recorded.												
35	20-Aug-12	U.S. District Court, Los Angeles California Los Angeles, California	A Los Angeles federal court clerk was identified as the source of leaked confidential information. The clerk was married to a convicted felon who then sold the information from sealed criminal case documents to an identity theft ring.	Internal spy	Database, information	Personal financial gain	Steal information	Theft/Exposure	x					Extra-legal, minor	https://www.fbi.gov/losangeles/press-releases/2013/former-federal-court-employee-and-husband-sentenced-for-leaking-confidential-court-records-to-tip-off-defendants-about-pending-arrests
36	24-Jun-12	Commodity Futures Trading Commission (CFTC) Washington, District Of Columbia	A CFTC employee received an email that linked to a fraudulent website. The employee failed to recognize the email as a phishing attempt and mistakenly entered information on the website. An unauthorized third party was then able to use the employee's account information to access emails and attachments that contained sensitive employee information such as names and Social Security numbers.	Employee reckless	Information	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://www.bloomberg.com/news/articles/2012-06-25/cftc-data-breach-risks-employees-social-security-numbers
37	22-May-15	United States Bureau of Justice Statistics (BJS) Washington, District Of Columbia	Hackers from Anonymous claim to have leaked 1.7 gigabytes of data belonging to the United States Bureau of Justice Statistics. The data file was posted on The Pirate Bay. It contained internal emails and the	Civil activist	server, information	Ideology	Change public opinion or corporate policy	Theft/Exposure, Operations impact, embarrassment	x	x	x	x		Extra-legal, minor	http://www.zdnet.com/article/anonymous-hacks-bureau-of-justice-leaks-1-7gb-of-data/

			website's entire database.												
38	11-May-12	California Department of Justice, Computer and Technology Crime High-Tech Response Team (CAT CH) San Diego, California	Email accounts of a retired agent for the California Department of Justice who was a member of a high-powered law enforcement computer security team in San Diego have been compromised by Anonymous, the infamous world-wide group of self-styled hacktivists.	Civil activist	private email accounts, information	Ideology	Change public opinion or corporate policy	Theft/Exposure, Operations impact, embarrassment	x	x	x	x		Extra-legal, minor	http://www.sandiegoreader.com/weblogs/news-ticker/2012/may/14/email-of-retired-government-security-agent-in-san-/#
39	27-Apr-12	Minnesota Department of Public Safety Driver and Vehicle Services St. Paul, Minnesota	An internal audit revealed that an employee at an unnamed Minnesota car dealership allowed an unauthorized friend to use his login information. It appears that the data was not used for criminal purposes.	Employee reckless	Information	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://www.twincities.com/ci_20496324/repo-worker-gained-illegal-access-minnesotans-motor-vehicle
40	3-Feb-12	Salt Lake City Police Department Salt Lake City, Utah	Hackers obtained police officer and non-police related civilian information from the Salt Lake City Police Department. The attack was in response to a proposed Utah bill that would have criminalized the possession of graffiti tools with the intent to deface property.	Civil activist	Information	Ideology	Change public opinion or corporate policy	Theft/Exposure, Operations impact, embarrassment	x	x	x	x		Extra-legal, minor	http://rt.com/usa/anonymous-hacker-kahuna-borell-779/
41	31-Dec-11	California Statewide Law Enforcement Association (CSLEA) Sacramento,	Hackers belonging to Anonymous group exposed the email addresses, passwords, and names of CSLEA members. The	Civil activist	Information including passwords and PII	Ideology	Change public opinion or corporate policy	Theft/Exposure, Operations impact, embarrassment	x	x	x	x		Extra-legal, minor	http://www.databreaches.net/california-statewide-law-enforcement-association-cslea-hacked/

		California	passwords were encrypted, but were posted in their decrypted form. The attack was politically motivated.													
42	15-Nov-11	The Public School Employees' Retirement System Harrisburg, Pennsylvania	About 2,000 pension fund members had their information placed online when an employee accidentally posted an unencrypted file on a public website. At least one person saw the information. The data breach occurred when an employee inadvertently posted an unencrypted file on a public website.	Employee reckless	Information	Accidental	No malicious intent	Theft/Exposure	x					Legal	http://articles.philly.com/2011-11-15/news/30401745_1_data-breach-security-breach-pension-fund
43	27-Oct-11	Ocala Police Department Ocala, Florida	A police officer was linked to a tax fraud ring. The officer accessed the Drivers And Vehicle Information Database (DAVID) in order to give the personal information of around 149 drivers to co-conspirators. The information was then used to open 184 bank accounts where fraudulent tax return checks could be cashed. An investigation was opened when the insider attempted to recruit someone else. The insider was suspended.	Internal spy	Database, information	Personal financial gain	Steal information	Theft/Exposure	x					Extra-legal, minor	http://www.databreaches.net/fl-ocala-police-officer-arrested-in-identity-theft-scheme/
44	14-Oct-11	Securities and Exchange Commission (SEC), Financial	FTT, a contractor working with SEC's ethics compliance program, violated its	Vendor reckless	Information	Accidental	No malicious intent	Theft/Exposure, Data loss, Op impact	x					Legal	http://www.reuters.com/article/2011/10/14/us-sec-databreach-

		Tracking Technologies (FTT) Washington, District Of Columbia	agreement with SEC by providing names and account numbers to a subcontractor, or subcontractors without permission. An SEC September 16 security review revealed that FTT had failed to comply with contractual obligations. The system was taken offline and FTT was told to terminate all third party access to SEC systems.												idUSTRE79D5O620111014 http://www.infosecurity-magazine.com/news/whos-watching-the-watchdog-sec-admits-to-possible/
45	14-Aug-11	Bay Area Rapid Transit (BART) San Francisco, California	Anonymous has claimed responsibility for a hack of BART's user database. A list with the first and last names, email addresses, passwords, phone numbers, full addresses and other personal information of MyBart.gov users was posted publicly. Anonymous exposed the security holes in BART's database in order to protest BART's temporary suspension of wireless service throughout BART stations.	Civil activist	Information	Ideology	Change public opinion or corporate policy	Theft/Exposure, Sabotage, Operations impact, embarrassment	x	x	x	x		Extra-legal, minor	http://www.theguardian.com/technology/2011/aug/15/anonymous-hackers-breach-bart-website http://mashable.com/2011/08/15/bart-anonymous-attack/
46	23-Jun-11	Arizona Department of Public Safety (AZDPS) Phoenix, Arizona	LulzSec has claimed responsibility for a hack of AZDPS. Hundreds of private intelligence bulletins, training manuals, personal email correspondence, names, phone numbers, addresses & passwords belonging to Arizona law enforcement and	Civil activist	Information	Ideology	Change public opinion or corporate policy	Theft/Exposure, Sabotage, Operations impact, embarrassment	x	x	x	x		Extra-legal, minor	http://www.azcentral.com/news/articles/2011/06/23/20110623lulzsec-hacks-into-arizona-dps-system-abrk23-ON.html

			spouses were released. LulzSec targeted the AZDPS in order to protest an Arizona policy they call racial profiling and anti-immigrant.												
47	5-Feb-11	Human Services Agency of San Francisco San Francisco, California	A former city employee emailed the information of her caseload to her personal computer, two attorneys and two union representatives. The former employee wanted proof that she was fired for low performance because she had been given an unusually high number of cases.	Employee disgruntled	Information	Disgruntlement	Damage or retribution	Sabotage, Embarrassment	x	x	x	x	x	Extra-legal, minor	http://www.workplaceprivacyreport.com/2011/02/articles/hipaa/employers-beware-aggrieved-employee-commits-data-breach-affecting-2400-individuals/ http://idt911.com/KnowledgeCenter/NewsAlerts/NewsAlertDetail.aspx?a=%7B3D678C9C-895D-4897-B345-974D77036012%7D

Appendix III

Interview Excerpts for tailored TAL & MOL

In this appendix, the interview structure and responses of the two experts from the interview conducted concerning the attributes, methods and objectives of threat agents for e-government infrastructures for businesses are described. Based on the exploratory study on Digipoort OTP, some specific threat agents (*End User Reckless, Fraudster, Vendor Reckless, and Certificate Service Provider*) were added to the tailored Threat Agent Library (TAL). The interview questions are mainly based directed at understanding the attributes, methods and objectives of these new agents. In addition to this, some questions are also related to the characteristics of already existing agents like *Mobster* – organized crime groups. We interviewed two experts, a Cyber Risk Services expert from a consultancy and an analyst in cyberattack research from a public organization. Both the interviewees are specialized in the public sector. The interview questions and the response of the two experts are shown below.

Responses of Security Expert 1

End User Reckless *End Users here are businesses or their intermediaries that connect to the e-government infrastructure to avail its services. End user related security behaviors are important for the information security effectiveness in organizations. Reckless End Users tend to by-pass safeguards for expediency, do not follow security protocols etc.*	
Effects	What can be the effects of end user recklessness on the e-government infrastructures? For e.g. Can it lead to theft/exposure of data, data loss, sabotage, operations impact, and/or embarrassment? *Purpose of the question: To identify whether the effect of reckless end users will be Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment.* **Ans:** All of that I would say. Reckless end user is a good differentiation between intentional and sloppiness of end users. There is not much difference between citizens or people working for a business. They could pick up malicious software, if the environment is not well maintained. Social engineering can lead to people clicking on malicious links which download malicious software. The effect is not that harmful for a service like OTP, but it can be. If someone makes malicious software that is targeted at e-govt then sloppiness can be a problem. *End user is a very relevant threat actor. Recklessness of End Users can lead to Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment.*
Methods	What could be the likely methods of attack on an e-government infrastructure due to a reckless end user? For e.g. Their actions could be copying or exposure of data, deletion of data, making the system unavailable, damaging or altering the system, taking or removing assets etc. *Purpose of the question: To understand the common methods/acts of a reckless end user. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** Different actors have different intentions. For recklessness, the typical effects are different from a targeted attack. By sloppiness, the disclosure of data is more likely than theft for instance. If someone makes an error in the technical infrastructure due to sloppiness, the services can become unavailable. In this case what is most likely is exposure of data, accidental deletion, or unavailability of the system. *Therefore, Copy/Expose is a likely method of attack, along with Destroy, Delete, Render unavailable.*

Fraudster *A Fraudster threat agent is defined here as an end user which misuses the system to perform Fraud.*	
Motivation	Considering that the end users here are businesses/intermediaries with considerable organizational resources, Organizational Gain is an important motivation to perform Fraud. What is the most important personal motivation for individuals involved in performing Fraud on behalf of the fraudulent organizations? *Purpose of the question: To identify the strongest personal motivation for individuals involved in Fraud, whether it is profit motive, pressure from peers, social pressures etc.* **Ans:** It's difficult to say in general. In general, the less harmful attacks are about proving yourself in the context of your peers. Real targeted attacks are different. An individual working for a business can be part of such criminal networks. In those cases, *the motivation is mainly financial gain*. That can be in many ways, for e.g. the fraudster can kidnap data too.
Objectives	What can be the objective of a Fraudster (businesses) to attack the e-government infrastructure for businesses? For instance, stealing valuable information, causing damage, destroying data, causing operations impact and/or embarrassment etc to the target organization. *Purpose of the question: To identify whether the objective of Fraudster will be Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment.* **Ans:** Financial gain is a primary motive. Stealing data can be a possibility, but more important is stealing access codes for e.g. DigiD codes. *Theft/Exposure of data is the most likely objective of a Fraudster.*
Methods	What could be the likely methods of attack by a Fraudster (businesses) on an e-government infrastructure? For e.g. Their actions could be to copy or expose valuable information, denying access to the system, deletion of data, making the system unavailable, damaging or altering the system, take or remove. *Purpose of the question: To understand the common methods/acts of a Fraudster. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** It depends on their motivations. If it's financial, theft of data of theft of access codes is most effective. If you talk about something like OTP, there is transaction information going through it. If the agent can modify this information, it can be useful. Then it's modification that is particularly interesting. For such a specific service like OTP, the agent needs specific information about the service. It's not really a secret, but not too much exposed like the DigiD. *Actions could be all of this, but stealing access codes is still more likely. Copy, Expose is the most likely method of attack here.*
Certificate Service Provider (CSP) *The CSPs issue digital certificates to the business customers & intermediaries on behalf of the PKIoverheid for connecting to various government services. E-government infrastructures use these certificates as a form of authentication while users connect over the internet. After the Diginotar incident, the importance of CSPs in the PKI is clearer. Here, the CSP is defined as a non-hostile threat agent, whose errors can impact the security of the e-government infrastructures.*	
Effects	CSPs could be non-trustworthy due to problems with issued certificates, errors in their systems, not following security protocols etc. What can be the effects of a non-trustworthy Certificate Service Provider on an e-government infrastructure? *Purpose of the question: To identify whether the effects of Certificate Service Provider errors will be Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment.* **Ans:** We have seen large effects from the Diginotar incident. The certificates were used in all

	parts of the e-govt infra. From the tax office, the border police, to the ministry of justice, *it affected in all kinds of ways*. The certificates had to be replaced. The other third parties were not ready to issue certificates immediately. *It caused significant operations impacts.* For several weeks there was a crisis team involved with the ministers heading it to resolve the issue. The certificates are usually used to maintain confidentiality, or authentication. Data loss was not really the issue. During the Diginotar, certificates were used by the Iranian authorities to eavesdrop into the communication of people. *Operations Impact is the most likely effect.*
Methods	What could be the likely methods of attack on an e-government infrastructure if the CSP is compromised? For e.g. Can it lead to exposure of data, deletion of data, unavailability of the system, damaging or altering the system, or taking/removing etc. *Purpose of the question: To understand the common methods/acts of a CSP. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** Certificates are used for all kinds of purposes of these days. Authentication of server side and client side. Client side certificates are not usually used for e-govt services, but that will change soon. *If a CSP is compromised, it could lead to copying/exposure of data.* Certificates are also used for electronic signatures. If certificates are flawed, the signature is not worth anymore. It sounds far-fetched but it's very much possible. It can lead to modifying of the data if certificates are flawed. *Copy, Expose and Damage, Alter are most likely here.*
Vendor Reckless *A vendor provides various services to e-government infrastructures. Some of these include development, monitoring and maintenance of the e-government infrastructure. Here, a vendor is defined as a business partner who provide services to the target organization, with a non-hostile intent, but who can still be a threat due to their reckless actions. Not following security protocols, circumventing safeguards etc can be reckless behaviour.*	
Effects	What can be the effects on an e-government infrastructure due to the recklessness of the service providing vendor? For e.g. For e.g. Can it lead to theft/exposure of data, data loss, sabotage, operations impact, and/or embarrassment? *Purpose of the question: To identify whether the effects of a Reckless Vendor will be Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment.* **Ans:** All of them. There are different types of vendors. If you buy a piece of software and there's an unintentional backdoor in it, there's a weakness in the system which can be exploited by someone with bad intentions. If you are a vendor who provides managed services for Logius, they can physically touch the infrastructure. Also the housing of the data center is by another provider. Someone from the vendor can switch it off, or use a stick and take data. It is very low tech. They can also remotely access the service, software and the data. They are there to manage the service, which means that they are able to touch it. That also means that if there's a database error, someone has to look into it to see what's wrong. Even when the data is encrypted, there's always someone who should have the key. Everything is possible, but some things are more likely. The physical and logical access as part of their job makes the impact higher. They could make mistakes, but they also have the most ability to abuse it. Therefore it is very important to select the vendor properly, and make sure that the vendor selects people who are trusted. Embarrassment is more a side effect here than an objective. In this case *I would say Theft/Exposure, Data Loss, and Operations impact.*
Methods	What could be the likely methods of attack on an e-government infrastructure due to a reckless vendor? For e.g. Can recklessness of the vendor lead to exposure of data, deletion of data, making the system unavailable, damaging or altering the system, taking or removing assets etc. *Purpose of the question: To understand the likely methods/acts of a reckless end user. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** The easiest way is someone with a lot of access rights, particularly someone like a

	database administrator. They have access to the database; they can read and modify it. That is often one of the largest risks. It is often bigger than the outside threats. So, everything depends on how reliable the person who manages a service is. The actions depend on the set up of the system. The attacks depend on the multi-tier infrastructure. Copying data is forbidden by a policy, but working from home is not. Vendors can work from home. He might need to manage the services remotely. The actions could be copy/exposure, deletion of data. Making the system unavailable is the biggest mistake and happens most often. It can be because the operator changed something by accident. For instance, while deploying something there was an error made, the system might stop working. So, unavailability can be a big possibility. Physically damaging the system is less likely. It's not usually irreversibly damaged. Take/ Remove are not likely. *Therefore I would say Copy/Expose, Destroy, Delete, Render unavailable and Damage, Alter (but not irreversible damage).*
Mobster *A mobster is a manager of an organized crime organization with significant resources. Their motivation could be organizational gain/personal financial gain. For e.g. extorting money by using ransomware, controlling, stealing, trading data etc.*	
Objectives	What can be the objective of a Mobster (an organized crime group) to attack the e-government infrastructure for businesses? For instance, stealing valuable information, causing damage, destroying data, causing operations impact and/or embarrassment etc to the target organization. *Purpose of the question: To identify whether the objective of Mobsters will be Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment.* **Ans:** The intention is financial gain, and the way to achieve it depends on the system that they are attacking. You can look at it from a data angle and from a business process angle. For e.g. requesting for a social benefit. If I can just misrepresent myself as someone else I can benefit from it. They look at easy ways to get the best gain. There are a lot of possibilities. Of course, high value and targeted attacks occur less often than low value, but they can succeed more easily with more resources. *Manipulation of data is very likely, for e.g. manipulating bank accounts, creating a fake transaction and inserting into the system can be interesting for OTP. Theft of information or confidentiality is overrated, unless it's the military.*
Methods	What could be the likely methods of attack by an organized crime group on an e-government infrastructure? For e.g. Their actions could be to copy or expose valuable information, denying access to the system, deletion of data, making the system unavailable, damaging or altering the system etc. *Purpose of the question: To understand the likely methods/acts of a Mobster. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** Logius provides infrastructural services. Both Logius and Belastingdienst have web portals. Abuse of software weaknesses in web portals is very common. It's related to modifying things to get access to data or to modify data. So it's related to damaging or altering the system. If someone wants data from e-govt infrastructures, they'll try to sell them. If you are a hacker, then they might put it on the internet for sale. *Copying/exposing, damaging/altering are likely. It is also possible to ask for a ransom*. DDOS has happened before on banks, government sites, Logius sites. It's possible but less likely, it is more difficult to sustain from an attackers point of view because they have to maintain a lot of volume and also the target are doing this. It's difficult to prevent, but they are less important than others.

Responses of Security Expert 2

End User Reckless *End Users here are businesses or their intermediaries that connect to the e-government infrastructure to avail its services. End user related security behaviors are important for the information security effectiveness in organizations. Reckless End Users tend to by-pass safeguards for expediency, do not follow security protocols etc.*	
Effects	What can be the effects of end user recklessness on the e-government infrastructures? For instance, can it lead to stealing or exposing valuable information; destroying or altering data; sabotage; causing operations impact; and/or embarrassment to the target organization. *Purpose of the question: To identify whether the effects of end user recklessness will be Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment.* **Ans:** *The main things are information leakage and embarrassment of the organization accordingly.* What you see and what you can pick up from the media is that reckless end users are not so much in sabotaging the systems because it is rather difficult to do if you are just reckless, but it is rather easy to get information and place them on the internet or your personal space which are connected to the internet. These cases happen fairly often. *Sabotaging hasn't been seen much often.* Sometimes, users think that he can access information easily on a special place for himself for efficiency, but doesn't realize that it's connected to the internet and doesn't think of the consequences. So it's reckless and sometimes choosing the easier way. In this case *it can lead to Theft/Exposure, Data Loss, and Operations Impact leading to embarrassment. Sabotage is not seen often.*
Methods	What could be the likely methods of attack on an e-government infrastructure due to a reckless end user? For instance, copy or expose valuable information; denying, withholding, or ransoming access to the system; destroying or deleting of data, making the system unavailable; damaging or altering the system; taking or removing assets. *Purpose of the question: To understand the likely methods of a reckless end user. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** *I would say only copying and exposing the information*. It is not a digital problem only, but the end user can print something from the environment, use it recklessly leading to exposure.
Fraudster *A Fraudster threat agent is defined here as an end user (businesses/intermediaries) which misuses the system to perform Fraud.*	
Motivation	Considering that the end users here are businesses/intermediaries with considerable organizational resources, Organizational Gain is an important motivation to perform Fraud. However, personal motivations of the individuals in the group are also important. What is the most likely personal motivation for individuals involved in performing Fraud on behalf of the fraudulent organizations? *Purpose of the question: To identify the strongest personal motivation for individuals involved in Fraud, whether it is profit motive, pressure from peers, social pressures etc.* **Ans:** *I think it is mainly profit motive*. If you see what happens in America with the tax payment organizations, those were end users fraudulently using, weakness in the application to get tax returns. *That is the first motivation that comes to mind.*
Objectives	What can be the objective of a Fraudster (businesses/intermediaries) to attack the e-government infrastructure for businesses? For instance, stealing or exposing valuable information; destroying or altering data; sabotage; causing operations impact; and/or embarrassment etc to the target organization.

	Purpose of the question: To identify whether the objective of Fraudster will be Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment. **Ans:** I will think that extracting information for personal gain is the main objective. So, mainly Theft/Exposure.
Methods	What could be the likely methods of attack by a Fraudster (businesses/intermediaries) on an e-government infrastructure? For instance, copy or expose valuable information; denying, withholding, or ransoming access to the system; destroying or deleting of data, making the system unavailable; damaging or altering the system; taking or removing assets. *Purpose of the question: To understand the likely methods of a Fraudster. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** I think *extracting of information mainly happens*. So I would say copy, exposing of information is a likely method.
Certificate Service Provider (CSP) *The CSPs issue digital certificates to the business customers & intermediaries on behalf of the PKIOverheid for connecting to various government services. E-government infrastructures use these certificates as a form of authentication while users connect over the internet. After the Diginotar incident, the importance of CSPs in the PKI is clearer. Here, the CSP is defined as a non-hostile threat agent, whose errors can impact the security of the e-government infrastructures.*	
Effects	CSPs could be non-trustworthy due to problems with issued certificates, errors in their systems, not following security protocols etc. What can be the effects of a non-trustworthy Certificate Service Provider on an e-government infrastructure? For instance, can it lead to stealing or exposing valuable information; destroying or altering data; sabotage; causing operations impact; and/or embarrassment etc to the target organization. *Purpose of the question: To identify whether the effects of Certificate Service Provider errors will be Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment.* **Ans:** The about the Diginotar affair makes me think about the availability of a service which uses a PKI. So, *Operations impact and embarrassment are the main effects. It can also lead to Data Loss, if someone uses falsified certificates. Theft/Exposure and Sabotage is not very likely.*
Methods	What could be the likely methods of attack on an e-government infrastructure if the CSP is compromised? For instance, copy or expose valuable information; denying, withholding, or ransoming access to the system; destroying or deleting of data, making the system unavailable; damaging or altering the system; taking or removing assets. *Purpose of the question: To understand the likely methods of a CSP. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** I would say the main thing is stealing information because when they work with false certificates, someone else can impersonate the user and get information by falsely authenticating. *Copying or Exposing is very likely in this case.*
Vendor Reckless *A vendor provides various services to e-government infrastructures. Some of these include development, monitoring and maintenance of the e-government infrastructure. Here, a vendor is defined as a business partner who provide services to the target organization, with a non-hostile intent, but who can still be a threat due to their reckless actions. Not following security protocols, circumventing safeguards etc can be reckless behavior.*	
Effects	What can be the effects on an e-government infrastructure due to the recklessness of the service providing vendor? For instance, can it lead to stealing or exposing valuable information; destroying or altering data; sabotage; causing operations impact; and/or embarrassment etc to the target organization. *Purpose of the question: To identify whether the effects of vendor recklessness will be*

	Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment. **Ans:** I would say *stealing information or espionage.* If an attack occurs through a vendor, something tells us then that you are doing extreme efforts not to be noticed. *If the vendor does not follow security protocols, it is easier to gain access to e-govt infrastructures through the vendors. It can also lead to data loss, and operations impact but the former is more likely.*
Methods	What could be the likely methods of attack on an e-government infrastructure due to a reckless vendor? For instance, copy or expose valuable information; denying, withholding, or ransoming access to the system; destroying or deleting of data, making the system unavailable; damaging or altering the system; taking or removing assets. *Purpose of the question: To understand the likely methods of a reckless end user. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** I would say that *copying or exposing is very likely*. Sabotage is less likely. Third parties can gain access to the e-government infrastructure through a vendor. A vendor could be well meaning, but not big on security. That is the most likely scenario. If you take the vendor as an actor *availability* problems can happen often in e-government structures due to the reckless vendor.
Mobster *A mobster is a manager of an organized crime organization with significant resources. Their motivation could be organizational gain/personal financial gain. For e.g. extorting money by using ransomware, controlling, stealing, trading data etc.*	
Objectives	What can be the objective of a Mobster (an organized crime group) to attack the e-government infrastructure for businesses? For instance, stealing or exposing valuable information; destroying or altering data; sabotage; causing operations impact; and/or embarrassment etc to the target organization. *Purpose of the question: To identify whether the objective of Mobsters will be Theft/exposure, Data Loss, Sabotage, Operations Impact, and/or Embarrassment.* **Ans:** I think all of them, *we see all of them*. They can attack the system for theft, data loss, extortion, sabotaging, embarrassing the company etc.
Methods	What could be the likely methods of attack by an organized crime group on an e-government infrastructure? For instance, copy or expose valuable information; denying, withholding, or ransoming access to the system; destroying or deleting of data, making the system unavailable; damaging or altering the system; taking or removing assets. *Purpose of the question: To understand the likely methods of a Mobster. It can include Copy, Expose, and Deny, Withhold, Ransom, and Destroy, Delete, Render unavailable, and Damage, Alter, and Take, Remove.* **Ans:** *We see all of them except taking or removing assets*. I would imagine it to be possible, but we don't see them very often. So it's less likely.

Results

Threat Agent	Characteristics	Security Expert 1	Security Expert 2	Values Selected
End User	**Effects**	*Theft/Exposure, Data Loss, Sabotage, Operations Impact, and Embarrassment*	*Theft/Exposure, Data Loss, Operations Impact, Embarrassment.*	*Theft/Exposure, Data Loss, Sabotage, Operations Impact, Embarrassment.*
	Methods	*Copy/Expose , Destroy, Delete, Render unavailable*	*Copy/Expose*	*Copy/Expose , Destroy, Delete, Render unavailable*

Threat Agent	Characteristics	Security Expert 1	Security Expert 2	Values Selected
Fraudster	**Motivation**	*Financial gain*	*Financial gain*	*Financial gain*
	Objectives	*Theft/Exposure*	*Theft/Exposure*	*Theft/Exposure*
	Methods	*Copy/Expose*	*Copy/Expose*	*Copy/Expose*
CSP	**Effects**	*Operations Impact*	*Data Loss, Operations Impact and Embarrassment*	*Data Loss, Operations Impact and Embarrassment*
	Methods	*Copy/Expose and Damage/Alter*	*Copy/Expose*	*Copy/Expose and Damage/Alter*
Vendor Reckless	**Effects**	*Theft/Exposure, Data Loss, and Operations impact*	*Theft/Exposure, Data Loss, and Operations impact*	*Theft/Exposure, Data Loss, and Operations impact*
	Methods	*Copy/Expose, Destroy/Delete/Render unavailable and Damage/Alter (less likely)*	*Copy/Expose, Destroy/Delete/Render unavailable*	*Copy/Expose, Destroy/Delete/Render unavailable*
Mobster	**Objectives**	*Theft/Exposure, Data Loss*	*Theft/Exposure, Data Loss, Sabotage, Operations Impact, and Embarrassment*	*Theft/Exposure, Data Loss, Sabotage, Operations Impact, and Embarrassment*
	Methods	*Copy/Expose, Deny/Withhold/ Ransom, and Damage/Alter*	*Copy/Expose, Deny/Withhold/ Ransom, Destroy/Delete/Render unavailable, and Damage/Alter*	*Copy/Expose, Deny/Withhold/ Ransom, Destroy/Delete/Render unavailable, and Damage/Alter*

Appendix IV
Interviews for Application

These interviews were performed as part of the application of TARA methodology in the case study on Digipoort PI in Chapter 7. Two sets of interviews were conducted. In the first set of interview, we used a tailored TAL (Figure 23) based questionnaire to understand the most relevant threat agents and the most critical assets of Digipoort PI. The relevance of the threat agents for Digipoort PI will be measured on an ordinal scale from 1 to 5, where 1 represents least relevance and 5 represents the highest relevance. The information from the interview will be used to prioritize the threat agents relevant to TAL and identifying the most critical assets of Digipoort PI. We interviewed Logius_Expert1, an expert in Digipoort PI for responses on the questionnaire. The questionnaire and the expert inputs are shown below. Table 25 shows a summary of the results from the questionnaire.

In the second set of interview, we interviewed the following experts to gather knowledge about the Key Management asset, its controls and exposures.

- Logius_Expert2, PKIOverheid
- Logius_Expert3, Certificate Manager, Digipoort
- Logius_Expert4, Incident Manager, Digipoort
- Logius_Expert5, Interim Ketenbeheerder, VENDOR1

The questions were specifically aimed at understanding the specific characteristics of the PKI of Digipoort PI, its implementation, accesses, security controls, and the likelihood of certain attack scenarios. Table 26 shows a summary of the responses of the experts.

Interview Set 1 – TAL Based Questionnaire

Scale for relevance from 1 to 5 (1 – least relevant and 5 – very relevant)

I. Identifying the critical assets

a) **What are the most critical assets of Digipoort PI and why?**

Digipoort PI is a secure infrastructure. For the access you need a key. The messages are encrypted over the channel, so to access the messages you need a key too. So, I think that the most critical assets are the keys and the *key management system*. It is otherwise called the Public Key Infrastructure (PKI). If that is compromised the threat agents could access Digipoort PI and the messages without detection. Therefore I think that they are the most critical assets.

Furthermore, the server is relatively open to the internet. So everybody who is connected to the internet and has a key can access Digipoort. Risks to the obvious assets like hardware, power supplies, physical connection lines etc can be mitigated by redundancy measures. They are directly monitored and easier mitigation measures exist for those assets. So, they are somewhat critical but threats to those assets will be noted directly, whereas threats to the key system cannot be directly noticed. That is why we should focus on the keys and the key management system as the critical assets.

II. Identifying the Relevant Threat Agents

1. End User Reckless

Relevance

a) On a scale from 1 to 5, how relevant do you think is reckless end use by businesses or intermediaries as a threat agent with respect to Digipoort PI?

I think they are very relevant. I would say 4. The end user is the user who has a valid key to the system, and who is using the critical asset. He is authenticated by the system using the key and can use the system in a valid way. If he does it recklessly, then he is the first threat agent to focus on.

b) What assets can be compromised by reckless end users? What would be the impact?

Within Digipoort PI are software processes. Those processes are what the end user use in the Digipoort. They can be compromised by reckless usage. The impact could be the loss of that process or loss of the entire system depending on the safeguards and the separation of the processes. I do not have insights into the compartmentalization of the process. But it is possible that the end user with the key can open doors to all the processes. It's a feature with a risk. You sign up as an end user for one process, SBR, or DigiInkoop, or UWA or any others. But by doing that he has access to all the other processes within the Digipoort PI. Within Digipoort PI he can use all the processes because it is one access system and one key to open the whole system. That again makes the key management system the most critical asset to be protected and safeguarded. The impact will depend on the compartmentalization of the processes. There can be operational impact. It can be small with some business impact or big with very high business impact.

2. Fraudster

Relevance

c) Do you think that end users are likely to perform fraud on Digipoort PI for organizational or personal gain? On a scale from 1 to 5, how relevant is an end user performing fraud as a threat agent for Digipoort PI?

The relevance for end user with a fraud mindset is less, may be a 2. This is because of the key management system. Every key authenticates the end user. If you access the system, the system knows exactly who it is using the digital certificate. A fraudster is immediately identified. So the end user is not likely to perform fraud on Digipoort PI.

d) What assets can be compromised by fraudulent end users? What would be the impact?

If a fraudster would want to compromise anything, it would be on the content and not the process. He would be interested in manipulating information like financial information, tax information etc. If the fraudster wants to commit tax fraud, he would probably try to compromise the tax office systems and not Digipoort.

3. CSP

Relevance

a) Would you say that there is a high chance of another Diginotar like incident happening which can impact the working of Digipoort PI? On a scale from 1 to 5, how relevant is a CSP as a threat agent for Digipoort PI?

I think that there were several new controls added since the DigiNotar affair to prevent it from happening. So, is it a threat agent? Yes it is definitely a threat agent. The relevance should be a 4 because as a threat agent CSP is still a very relevant threat agent even though controls have been strengthened.

b) What assets of Digipoort PI can be compromised by an incident similar to Diginotar? What would be the impact?

The key management system could be completely compromised similar to DigiNotar. The impact would be the business impact involved in reissuing the keys. Every end user will have to be re-issued the keys. There will be a big downtime for business.

4. Vendor

Relevance

a) On a scale from 1 to 5, how relevant is a Vendor (External/Internal) acting recklessly as a threat agent for Digipoort PI?

There are two main external vendors - VENDOR1 and VENDOR2 and two main internal vendors – MS and CvS. I would give a definite 5 for VENDOR1 and VENDOR2 with respect to the critical assets. I would consider the relevance of an external vendor as a threat agent the highest, even higher than an end user. The reason for this is because the vendor is the one who manages the system. They adapt, perform releases, and monitor the system. If they do it wrong, the whole system could collapse. So the reckless vendor is of highest relevance.

VENDOR2 manages the underlying infrastructure. I would say the relevance is once again high. The relevance is a 5. The system is in a datacenter. If the datacenter is done poorly, a reckless behavior, things could go wrong.

As far as internal vendors are concerned, I would give them less relevance as a threat agent. MS has no real access to the Digipoort system, their reckless behavior is only in process management. The impact would be that a wrong issue or problem could be prioritized. CvS do not access the system directly too. They mainly manage the data taxonomy. So I would say a relevance of 2 would be justified for internal vendors. No assets are directly affected by the internal vendors.

b) What assets can be compromised by a reckless vendor? What would be the impact?

Assets that can be compromised are different. The software is one. With new releases there are sometimes problems with the different parts of the system not working due to recklessness in the releasing of the software by VENDOR1. The impact to this can be partial unavailability.

Another asset is the underlying infrastructure managed by VENDOR2. VENDOR2 also manages the servers. If there's a reckless behavior, it could lead to total unavailability and very high business impact.

c) **On a scale from 1 to 5, how relevant is a Vendor (External/Internal) acting intentionally as a threat agent for Digipoort PI?**
I don't think a vendor acting intentionally against us is relevant, although employee disgruntlement at the vendor seems relevant.

d) **What assets can be compromised by the hostile action of a vendor? What would be the impact?**
I think the same assets we mentioned in the question b) can be compromised. But this would of course be during the operational time. Outside the service time of the vendor, the old vendor will not have any access.

5. Employee Disgruntled, Reckless & Error

Relevance

a) **On a scale from 1 to 5, how relevant are insider threats (especially disgruntled employees, employee recklessness & employee errors) on Digipoort PI? Please tell me the relevance score that you would give for each of these threat agents.**
Employees could be of different types, employees of Logius, vendor employees, CSP employees etc.
I would say that all the employee threat agent archetypes have a relevance of 3 if they are Logius employees. The employees of Logius cannot access the code, but they have insights about the system. The impact would be the same, so the relevance is also the same for these three threat agent archetypes. The relevance is not the highest for Logius employees because of the lack of direct access. An ex-employee would have an even lower relevance (may be a 2).
The employee archetypes of the vendor have higher relevance because they have deeper access to the system. Real disgruntled active vendor employees are the highest threat agent because they have internal access. They could pull the plug and we will have a huge impact. Or a wrongly placed semicolon on the code can also have a huge impact.

b) **What assets can be compromised by these threats? What would be the impact?**
The asset Logius employees could compromise the confidentiality of the process. That information could be the asset that can be compromised by Logius employees. This could lead to higher vulnerability. If the confidential information is exposed it could increase the vulnerability of the system. Vendor employees could expose the whole system, hardware, software depending on the type of vendor they are.

6. Civil Activists & Foreign Government Spies

Relevance

a) **Can Digipoort PI be hacked?**
I cannot say no. But, the Digipoort PI does not hold any information. It's a postman. The biggest threat from these agents could be DDOS attacks.

b) **Can the information flow through Digipoort PI be used by foreign governments, or other ideological hacker groups to gain illicit advantage over the Dutch government or the businesses?**

On a scale from 1 to 5, how would you rate the relevance of these threat agents for Digipoort PI?

All the tax information of all the companies in the Netherlands goes through the Digipoort PI. That information is confidential. The content is therefore definitely interesting for these external parties. The Digipoort PI is made to withstand threats from external agents like these. So, the relevance as a threat agent for these actors against Digipoort PI is very low. It can be even a 1. For instance, if a foreign agency wants to access the system, then you have to have a key and it has to be valid. So it can't be done covertly. Therefore they have information that could be useful for them, but attacks from these threat agents are not really relevant for Digipoort PI.

c) What assets can be compromised by these threats? What would be the impact?

It depends on their objective. If they perform a DDOS, then they can compromise the availability of Digipoort which is an important asset. The impact would be business impact.

7. Mobsters & Internal spies

Relevance

a) Can the information flowing through Digipoort PI be used by organized crime groups for financial gain through external access of Digipoort PI? If yes, how relevant is this threat agent for Digipoort PI on a scale from 1 to 5?

No, they cannot access the information without a key because the information is encrypted. The information itself could be interesting for blackmail or ransoming. But because they don't have internal access their relevance as a threat agent is low. If I was a mobster and I wanted to get this information, I would try to hack where the information goes into the system (the system of the businesses) or from where it comes out of the system (the tax office). So, for Digipoort PI this threat agent is not very relevant. I would say a 1 for the relevance score.

b) What assets can be compromised by a threat agent through external access? What would be the impact?

Availability could be the asset that can be compromised. Otherwise I don't see any other assets that can be compromised.

c) How easily can the information flowing through Digipoort PI be used by an actor with internal access for financial gain? How relevant are internal spies as a threat agent for Digipoort PI on a scale from 1 to 5?

It is somewhat relevant because the threat agent has internal access. So, I would say a 3. The easiness with which an Internal Spy can access valuable information from Digipoort PI would depend on where the threat agent is; at the vendor side it is easier. At the Logius side it is not very easy but not impossible.

d) What assets can be compromised by a threat agent through internal access? What would be the impact?

I would say, mainly the information. The data in the envelope is valuable to some groups of people. If the internal spy were to sell this data to a mobster then the confidentiality of Digipoort will be violated. So, no asset of the Digipoort PI itself, but the confidentiality of Digipoort PI could be violated. The impact could be financial losses, embarrassment etc.

7. Thief (Internal/External)

Relevance

a) Have there been cases of physical theft in the past? If yes, was it a burglary or internal theft? How would you rate this threat agent on a relevance scale from 1 to 5 with respect to Digipoort PI?

I do not know if there have been cases of theft in the past. But, a burglar has no relevance. Internal theft could be relevant but really low, may be a 1.

b) What assets can be compromised by a thief with internal access? What would be the impact?

The most valuable assets could be the keys which could be contained in the hardware. But that is near to impossible because of the high security associated with storing keys. The impacts would be impersonating an end user.

c) What assets can be compromised by a burglar? What would be the impact?

They could take hardware, but it won't have much of an impact.

III. Remarks

a) Is there anything else you would like to share on this topic? Is there any other threat agent that you would like to add to the library?

I think this is sufficient with respect to Digipoort PI. However, I feel that it would be nice to have sub classifications of employees depending upon their roles. I think this methodology is an interesting way of looking at the system. What would help is a way to make a self-explanatory questionnaire. If I have a closer look at the Threat Agent Library (TAL), I might be able to do it myself.

Results of Interview Set 1

Table 25: Results of the questionnaire

Threat Agent	Description	Relevance Score (1 - least relevant to 5 - very relevant)	Critical Assets Compromisable	Impact
End User Reckless	Users of Digipoort PI (businesses/HUBs) who can cause unintentional damage to the system, due to their reckless behavior or carelessness.	4	Process Infrastructure	Low to high business impact due unavailability of the process infrastructure.
Fraudster	Users of Digipoort PI (businesses/HUBs) who	2	Information, Confidentiality of Digipoort PI	Low impact, because the user

Threat Agent	Description	Relevance Score (1 - least relevant to 5 - very relevant)	Critical Assets Compromisable	Impact
	intentionally attempts to access the information in the system, to perform fraud.			is easily identifiable with the key and the information is encrypted.
CSP	Third party certificate providers for the Public Key Infrastructure (PKI), who provides keys or certificates to the users. Errors made by CSPs can have a big impact on the Digipoort PI system.	4	Key management system or the PKI	High business impact due to unavailability of the system.
Vendor Reckless	Service providers of Digipoort PI with internal access, and acting in a reckless or careless manner. Includes also employee recklessness or error at the vendor.	5	Software, and hardware assets	1. Partial unavailability and business impact due to software error. 2. Total unavailability and high business impact due to hardware problems.
Vendor (Hostile)	Service providers of Digipoort PI with internal access, trying to gain business or financial advantage through hostile actions. For e.g. using inside information.	-	Software, and hardware assets	Unavailability and business impact.
Employee Disgruntled - Logius	Current or former employees of Logius with intent to harm the organization.	3	Information, Confidentiality of the process	Increased vulnerability of the system
Employee Disgruntled - Vendor	Current or former employees of Vendors with intent to harm the organization.	4	Software, and hardware assets	Total unavailability and high business impact due to compromise of the software or the hardware.
Employee Reckless - Logius	A non-malicious current employee of Logius who circumvents safeguards for expediency.	3	Information, Confidentiality of Digipoort PI	Increased vulnerability of the system
Employee Error - Logius	A non-malicious current employee of Logius, who follows poor processes, makes unforeseen mistakes, or simple mistakes.	3	Information, Confidentiality of Digipoort PI	Increased vulnerability of the system
Civil Activists	A highly motivated but non-violent supporter of a	1	Confidentiality/Availability of Digipoort PI	Low business impact

Threat Agent	Description	Relevance Score (1 - least relevant to 5 - very relevant)	Critical Assets Compromisable	Impact
	cause trying to access Digipoort PI for ideological motives.			
Foreign Government Spy	Foreign state backed actors who spy on the confidential data of other governments or government agencies.	1	Confidentiality/Availability of Digipoort PI	Low business impact
Mobster	The manager of an organized crime organization with significant resources trying to access Digipoort PI for organizational or financial gain.	1	Availability of Digipoort PI	Low business impact
Internal Spy	A trusted insider who gathers data with a simple profit motive. They lead to the theft of IP, PII, or business data.	3	Information, Confidentiality of Digipoort PI	Financial losses, Reputation damage
Thief (External)	An opportunistic individual with a simple profit motive, with external access, usually a burglar.	-	Hardware containing keys	Low impact due to the high security associated with storing keys
Thief (Internal)	An opportunistic individual with a simple profit motive, with internal access, usually an employee.	1	Hardware containing keys	Low impact due to the high security associated with storing keys

Interview Set 2 – PKI of Digipoort PI

I. Key Management System Asset – General

a) What are the main components of Digipoort Key Management?

Logius_Expert3: Digipoort is a lot of processes for and there might be certificates within some processes too. I do not exactly know where, that is more from an architectural point of view. I am more involved in buying the certificates for Digipoort PI as the Certification Manager. Logius manages Digipoort with our suppliers. VENDOR1 generates the keys (public and private keys) in the servers. A CSR (Certificate Signing Request) file is also generated by VENDOR1 with the public key. The CSR file is sent to the Certificate Manager at Logius, who files it with the CSP for signing. When the certificate is validated, the Certificate Manager downloads the CSP validated CER (a file extension for a certificate) file and sends it to VENDOR1 via email for installation in the servers. They use some software (do not exactly know what) to install the certificates into the servers which are hosted by VENDOR2.

The Certificate Manager purchases the certificates from the CSPs like QuoVadis, KPN, or Digidentity using a Certificate Signing Request (CSR). Once the certificates are ready, I will download them from the respective CSP portals by signing in with a username and password usually. With QuoVadis, a

token is also used for signing in. So QuoVadis is more secure. Once I download the CER file on to my computer in a PEM format I will send it by email to our supplier VENDOR1. They will install it into the servers of Digipoort PI.

b) Who has access to the Key Management asset, especially the private key?

Logius_Expert3: Our supplier VENDOR1 generates the private key and public key for Digipoort PI. The private key is stored securely in the server in which it is generated. They have to use multiple authentications using username, password and tokens to install something in the server. It is not easy to get access to the server. In addition to this, there's more than one administrator involved in maintaining the system. VENDOR2 servers are housed in a much closed system. Nobody can get into the server rooms easily; they have strong perimeter controls including finger print scanning.

c) Does the KMS of services like Digipoort use the OCSP (Online Certificate Service Protocol) for checking CRL every time?

Logius_Expert3: We do not use the OCSP to check the CRL in real time. We download the updated CRL every four hours from the CSP. Therefore if a certificate is revoked by the CSP, within 4 hours after the certificate will be refused for communication by Digipoort PI.

d) VENDOR1 with the support of VENDOR2 installs and manages the certificates for Digipoort PI. What controls exist to ensure that the vendors are doing the key management properly?

VENDOR1 and VENDOR2 must be ISO certified, which they are. Therefore we know that they are following the processes. Logius is BIR compliant and is moving toward ISO certified. There's also communication between KD and MS (Managed Services). MS talks to VENDOR2 and KD talks to VENDOR1. We don't talk directly with VENDOR2. So MS will check VENDOR2 about the processes to make sure that things are working properly. At KD we are responsible for ensuring that things are going well with VENDOR1. If there's something between VENDOR1 and VENDOR2, the KD manager talks with MS manager.

II. Attack Scenarios - CSP

a) The private key of a CSP is compromised due to lack of minimum security controls like strong passwords, or an anti-virus on the cryptographic modules of the CSP. The certificates issued to Digipoort PI cannot be trusted anymore and all the keys have to be replaced. Is this a likely scenario?

Logius_Expert2: Highly unlikely because of the strong requirements for network security, the external auditors are more poised than ever, we also visit them now for audits. It is highly unlikely but can happen. The baseline requirements is an international standard that has to be adhered to, otherwise browsers do not accept the root certificate. In addition to his the CSPs also have to adhere to the network guidelines. So, multi-factor authentication for PKI services is necessary. The controls implemented make it unlikely now.

b) A CSP erroneously issues certificates that are meant to be user certificates, but turn out to be intermediate CA certificates. An attacker misuses the intermediate certificate to generate rogue

certificates for accessing the Digipoort system. The CSP later realizes this mistake and revokes the certificate. Should the key pair of Digipoort be replaced because of this attack?

Logius_Expert2: This shouldn't happen, if this happens we will get into a lot of difficulty. Normally CSPs are not allowed to issue intermediate certificates. But we are planning to implement that down the line in generation 3. Two CSPs of the seven can create sub CAs, Digidentity (commercial) and CIBG (govt). But they are not allowed to create additional sub-CAs without notifying us. They are also audited. So, this is highly unlikely.

c) **The CSP did not include a link to the CRL location for revocation checking in the user certificates. Digipoort PI continues to communicate with a revoked certificate. Can it lead to a possible exposure of the keys of Digipoort PI?**

Logius_Expert2: This is unlikely too, because all the requirements mandate that there should be a CRL endpoint in it. Moreover they use a template. If there's no CRL endpoint, Digipoort PI has a softfail, which means that they probably use the certificate anyways. OTP on the other hand has a hard fail and refuses the connection.

d) **The OCSP is not maintained properly by the CSP. The updated CRL list cannot be accessed by the key management system of Digipoort PI in real time. This leads to wrongful authentication of users and possible exposure of the keys of Digipoort PI and damage to the key management system. Is this a likely scenario?**

Logius_Expert2: The OCSP is not checked online. They download the CRL and use it to check the revocation status. The CRL has a validity of 48 hours and downloads a new CRL every 4 hours. It cannot cause any damage to the keys of Digipoort PI.

III. Attack Scenarios – Logius Employees

a) **As a disgruntled employee at Logius what can you do to attack the key management system (expose, damage, make unavailable, alter, take)?**

Logius_Expert3: It's very difficult as a certification manager to attack the system. If I revoke a certificate, it's from my own account. So, I will be easily tracked. There's more risk with disgruntled employees at the VENDOR1 side. But there also the duties are distributed, like more than one administrators etc.

b) **Can you just give the certificate to someone else? The certificate managers can download the key from the CSP. What if you just sent it to someone else?**

Logius_Expert3: It's difficult. If I buy the certificate, the CSP must receive the money. The order of the certificate will be in the financial system (DigiInkoop). The order is managed by several people in the KD who must be in accordance with the order. There's a URL in the certificate which is exactly for the URL of the server. If someone else uses the certificate, it won't work.

c) **What if an employee with access to the key (like the Certificate Manager) decides to leave Logius and is going to share this confidential information with an outsider?**

Logius_Expert3: I have to contact all the CSPs and inform them that I am no longer working with Logius to let them know that I am not working with Logius anymore so that they can disable my permissions. It is also the responsibility of the team leader. The team leader will make sure that the permissions are revoked. It will also be communicated to the PKIOverheid.

d) How do you take responsibility of your passwords and credentials?
Logius_Expert3: Nobody else has access to my documents or passwords. All the data from vendors are password protected for regulating access. All the documents for me are only available to me.

e) Did you receive any training against SE attacks?
Logius_Expert3: Yes. I have had training in ISO 27001 and is ISO 27001 certified. I also did an internal Belastingdienst academy training for information security.

f) Are there regular audits happening for certificate and key management?
Logius_Expert3: Yes. We are BIR compliant. We audit the processes with the information security team. We are working towards ISO certification.

g) What could be a fatal error from your side with respect to the Key Management system?
Logius_Expert3: If something happens, I have to contact PKIOverheid, and my managers. I have been a certificate manager for one year; there have been few errors involved. If I send the PEM file unknowingly to someone else by error, I can revoke the certificate and get the new certificate on the same order number. The CSP will give the new certificate without any extra cost. I can revoke the certificate very quickly and very easily if I made an error in sending it to someone. One error that was made was regarding a specific field in the CSR which led to some wrong certificates (CER files) being issued by the CSP. But, it was not high priority. I revoked the certificate and contacted the CSP to understand why the certificate was created in spite of the error in the entry.

h) What controls are implemented to prevent errors in issuing certificates?
Logius_Expert4: I do a CSR control on the CSR files before they are sent to the CSPs for signing. If something unusual comes up, I inform the Certificate Manager in charge of it. We then ask the vendor to reissue a CSR.

i) What if the error went undetected and VENDOR1 implemented the wrong certificates?
Logius_Expert4: In that case we would have had an interruption in the production for only a short period. This is because all the certificates of Digipoort have a primary certificate and a back-up certificate. So they would've had to install the back-up certificate.

IV. Attack Scenarios – Vendors

a) How many administrators at VENDOR1 have access to the key management system? How is access regulated (authentication, logging and monitoring etc)? Are the duties of an administrator distributed among multiple employees to avoid dependence on a single employee?
Logius_Expert5: There are at least two administrators who can access the key management system. This is for security purposes and also to ensure that no one person is fully in control of the asset. The access list of administrators is also handled by the Managed Services department of Logius.

b) Do employees at VENDOR2 provide any services related to the key management and have access to it? How is access regulated?

Logius_Expert5: No. The job of VENDOR2 is to host the Digipoort service. They are the suppliers of the hard-ware. The keys are installed in the servers of Digipoort PI. The servers are physically housed in the datacenters of VENDOR2.

Logius_Expert3: Employees at VENDOR2 might not have any idea as to the particular hardware on which Digipoort is hosted. I have visited VENDOR2 datacenters multiple times. It is a very heavily secure facility. Servers of facebook, the CERN etc are hosted there. The datacenter building is surrounded by a moat, and has tall walls. If you want to enter the facility you have to give a proper identification using your passport. It is not easy for an external actor to enter the VENDOR2 facility. There are several floors of servers. It is not easy to understand which server is where. The access is restricted to administrators using passwords, keys, hand scanning etc. Furthermore, there are also other restrictions for the administrators of VENDOR2, like multiple administrators etc. VENDOR1 and VENDOR2 works together, but the physical business is separated from the software. VENDOR1 communicates mainly with the KD and VENDOR2 communicates mainly with MS. The coordination of the two suppliers is performed through the communication between KD and MS. This helps Logius in maintaining control as the SSC.

c) Mr. X is an administrator at VENDOR1. He wrote down the password to the key server on a piece of paper for convenience. The paper wasn't shredded and ended up in the dumpster. A dumpster diving actor obtains the access credentials to the key server as a result. This could lead to the compromise of the key server and exposure of the private key. Is this a likely scenario? What controls are implemented to prevent this scenario?

Logius_Expert5: No. Nobody writes their password on a piece of paper. If an administrator is caught with a password on a piece of paper, he will most likely fired on the spot.

d) Mr. X is an employee of VENDOR1. A social engineering attacker tricks Mr. X into using a malware affected USB stick on the computer connected to the key server. The malware compromises the server and leads to exposure of the private key of Digipoort PI. Is this a likely scenario? What controls are implemented to prevent this scenario (any training for employees)?

Logius_Expert5: VENDOR1 takes responsibility to prevent such attacks. How they handle this is beyond me.

e) A public certificate was issued by the CSP using a wrong CSR that was generated by the VENDOR1 server. The Certificate Manager at Logius did not identify the error in the CER file and sends it to VENDOR1 for installation in the server. Will VENDOR1 install the certificates or do they conduct checks to ensure that the certificates are according to standards? If the certificates are installed, will the error be detected before it goes in production?

Logius_Expert5: There are tools for checking the correctness of the CSR. In addition to this, the hash values of the new certificates are also checked to see whether the certificates were modified or are wrong.

f) An employee at VENDOR2 accidentally lets an unauthorized person tailgate into the building where the key server is housed. The person accesses the server and manages to steal the private key from the server. Is this a likely scenario?

Logius_Expert3: This does not happen due to the strict security. Refer to Q.9.

g) What if an employee with admin access to the key server decides to leave VENDOR1? Can he misuse his permissions or knowledge of the system once he leaves VENDOR1?

Logius_Expert5: As soon as an employee is relieved of his duties, all his accesses and permissions are revoked. They will not have accounts anymore. Therefore he cannot misuse any of the permissions he had based on his role.

h) A disgruntled employee at VENDOR1 has access to the server in which the private key of Digipoort PI is stored. He shares his access credential information with an external attacker. External attackers misuse credentials to steal the private key stored in the server (possibly over the network). The key system is compromised and communications are insecure. Logius now has to revoke the certificates. VENDOR1 has to generate new keys and get new digital certificates from the CSP. Is this a likely scenario? What controls are implemented to prevent this scenario?

Logius_Expert5: This scenario is unlikely. In addition to this, we also have 2 sets of certificates. This enables us to block the compromised certificates and activate the back-up certificates.

i) A disgruntled administrator at VENDOR1 disables the anti-virus application on the key server. The key server is now unprotected and could become vulnerable to external attackers. Is this a likely scenario? What controls are implemented to prevent this scenario?

Logius_Expert5: This is not likely. There's more than one administrator for the server. Any change will be easily detected. Moreover, any changes to the system should be reviewed and approved by the KD.

j) Former administrator employee at VENDOR1 is disgruntled. He shares his access credentials and details regarding the implementation and location of the keys of Digipoort PI in the server to an external entity .The attacker now clearly knows where to look for in the server to copy the keys of Digipoort PI. What controls are implemented to prevent this scenario?

Logius_Expert5: The credentials are being blocked immediately. It is useless to share his access credentials.

k) Administrator employee at VENDOR2 is disgruntled and shares confidential information like the make and type of server used for storing the private key of Digipoort PI to hostile actors. The hostile actors try to physically access the server in which the key is stored. This can jeopardize the security of the private key of Digipoort PI. Is this a likely scenario?

Logius_Expert5: VENDOR2 servers are hosted in a high security infrastructure. It is not possible to access the servers even with such information.

V. Attack Scenarios – Internal Spy

a) If I was a very highly skilled person in spying on cryptographic information at Logius/VENDOR1/VENDOR2, how easily can I get my hands (as a non-administrator) on the private key or an access password to the key?

Logius_Expert3: From Logius, it is not really possible. There's more likeliness if the spy is in VENDOR1. VENDOR2 has no idea about the information in the servers. At VENDOR1, the private key information can be obtained by accessing the server. However, the VENDOR1 network is secure. You have to get a log in, you have to get a token. The administrators log in with a password and a token. There are multiple administrators (at least two). At VENDOR2, it's not physically possible to access the servers. They have a high perimeter security with surveillance, finger print logging etc.

b) If someone compromises Diginetwerk using malware will he get some crucial information about the private key?

Logius_Expert3: No, the Diginetwerk is secure. There's compartmentalization. Everything that you do on the network is traceable. There is reporting, log-ins, firewalls in place. You cannot just plug a USB on the laptop and install something on the network.

Results of Interview Set 2

Table 26: Knowledge about Key Management of Digipoort PI

Components of Key Management System	• Logius manages Digipoort with our suppliers. VENDOR1 generates the keys (public and private keys) in the servers. A CSR (Certificate Signing Request) file is also generated by VENDOR1 with the public key. The CSR file is sent to the Certificate Manager at Logius, who files it with the CSP for signing. When the certificate is validated, the Certificate Manager downloads the CSP validated CER (a file extension for a certificate) file and sends it to VENDOR1 via email for installation in the servers. They use some software (do not exactly know what) to install the certificates into the servers which are hosted by VENDOR2. • We do not use the OCSP to check the CRL in real time. We download the updated CRL every four hours from the CSP. Therefore if a certificate is revoked by the CSP, within 4 hours after the certificate will be refused for communication by Digipoort PI.	Logius_Expert3
Access to Key Management System	• The private key is stored securely in the server in which it is generated by VENDOR1. They have to use multiple authentications using username, password and tokens to install something in the server. In addition to this, there's more than one administrator involved in maintaining the system. • VENDOR2 servers are housed in a much closed system. Nobody can get into the server rooms easily; they have strong perimeter controls including finger print scanning.	Logius_Expert3
CSP	• It is highly unlikely that the private key of CSP will be compromised. Scenario a (Table 20) is therefore highly unlikely. • Normally CSPs are not allowed to issue intermediate certificates. They are also audited. So, scenario b is highly unlikely. • All the requirements mandate that there should be a CRL endpoint in it. Moreover they use a template. So, scenario c is highly unlikely. • The OCSP is not checked online. They download the CRL and use it to check the revocation status. There's no damage to the private key of Digipoort PI. Scenario d is therefore unlikely.	Logius_Expert2
Logius Employees	• A certification manager cannot attack the system easily due to the lack of access to the private key and monitoring of activities.	Logius_Expert3 Logius_Expert4

	• The certificate ordering process is managed through the DigiInkoop. There's also a URL in the certificate which is exactly for the URL of the server. If someone else uses the certificate, it won't work. • When a certification manager leaves Logius, the responsible persons are notified and accesses are revoked. • Access to documents are strictly restricted using passwords and tokens. • The certification manager received training in ISO 27001 and internal Belastingdienst academy training for information security. • The systems are BIR compliant. Internal audits are also conducted. • Errors in CSR files occur due to mistakes from VENDOR1. But these errors can be easily rectified. • CSR control is performed to prevent errors in certificates. In addition to this, all the certificates of Digipoort have a primary certificate and a backup certificate.	
Vendors	• There are at least two administrators who can access the key management system. This is for security purposes and also to ensure that no one person is fully in control of the asset. • VENDOR2 supplies hardware. They do not have any direct logical access to the keys of Digipoort PI. VENDOR2 servers are also highly secure. • VENDOR1 and VENDOR2 works together, but the physical business is separated from the software. VENDOR1 communicates mainly with the KD and VENDOR2 communicates mainly with MS. The coordination of the two suppliers is performed through the communication between KD and MS. This helps Logius in maintaining control as the SSC. • Reckless behaviour is not tolerated at VENDOR1. Misuse of passwords, tailgating etc does not happen. • The correctness of CSR's are checked using tools. In addition to this, the hash value of the certificates is also checked before installation. • Accesses and permissions of an ex-employee are immediately revoked at VENDOR1. • Any change to the system should be reviewed and approved by the KD. Modification of existing applications or installations of new applications are therefore not possible.	Logius_Expert5
Internal Spy	• An internal spy at Logius cannot do much. The Diginetwerk is secure. There's compartmentalization. Everything that you do on the network is traceable. There is reporting, log-ins, firewalls in place. You cannot just plug a USB on the laptop and install something on the network. • Internal spies will have better success at VENDOR1. At VENDOR1, the private key information can be obtained by accessing the server. However, the VENDOR1 network is secure and access is regulated. At VENDOR2, it's not physically possible to access the servers.	Logius_Expert3

Appendix V

In Chapter 7 we demonstrated the application of TARA methodology to the *Key Management* asset. Here we discuss the results of applying the TARA methodology in a broader manner to the other assets of Digipoort PI. First, we discuss the outputs of Step 1 - the critical assets, the prioritized list of threat agents, and their likely methods and objectives. Then we discuss the outputs of Step 2 – the sample attack scenarios of the threat agents, and the controls and exposures of Digipoort PI. Subsequently, we summarize the threat landscape of Digipoort PI.

Step 1: Filter and Prioritize Threat Agents, Objectives and Methods.

Critical assets and prioritized list of threat agents

All the relevant threat agents for Digipoort PI, the assets that could be compromised by these threat agents and their potential impacts were shown in the prioritized list of threat agents in Table 17.

Likely Methods & Objectives

We looked at the tailored MOL (Figure 24) to find out the methods and the objectives that are associated with the threat agents in Table 17. We have highlighted the likely methods of attack for each threat agent on the various assets. This is explained more in the following step.

Table 27: Prioritized Threat Agents, Objectives, Methods and Assets

			Methods					Assets			
Threat Agent	**Motivation**	**Objectives**	Copy, Expose	Deny, Withhold, Ransom	Destroy, Delete, Render Unavailable	Damage, Alter	Take, Remove	Process Infrastructure	Software	Hardware	Information
End User Reckless	Accidental	No malicious intent	x		x			x			
CSP	Accidental	No malicious intent	x			x					
Vendor Reckless	Accidental	No malicious intent	x		x				x	x	
Employee Disgruntled - Logius	Disgruntlement	Sabotage, Embarrassment	x	x	x	x	x				x
Employee Disgruntled - Vendor	Disgruntlement	Sabotage, Embarrassment	x	x	x	x	x		x	x	
Employee Reckless - Logius	Accidental	No malicious intent	x		x	x					x

Employee Error - Logius	Accidental	No malicious intent	x		x	x					x
Internal Spy	Personal Financial Gain	Theft/Exposure	x								x

Step 2: Identifying Vulnerabilities and Exposures for Digipoort PI

Likely Attack Scenarios

By focusing on the characteristics of the assets, we have highlighted the likely methods of attacks for each threat agent as shown in Table 27. For instance, the *Process Infrastructure* asset is a set of processes in the Digipoort infrastructure corresponding to the various government agencies. This asset is more likely to be rendered unavailable than be copied or exposed by the recklessness of an end user. Based on this, we created the following sample attack scenarios on the *Process Infrastructure* asset.

End User Reckless

a) Username and password of an end user were compromised as a result of poor security practices at the end user leading to a DDOS attack on Digipoort PI.
b) Poor security practices led to theft of digital certificates from the client server which is used by an attacker to send information to Digipoort PI.

For the *Software and Hardware* assets of Digipoort PI, recklessness or a disgruntled employee at the Vendor can be a very relevant threat agent. Vendor Recklessness can cause the exposure of information or unavailability of the software or hardware assets. A disgruntled employee at the Vendor has a higher relevance than a disgruntled employee at Logius. This is due to the formers direct physical access to the software or hardware assets. We created the following sample attack scenarios on the *Software and Hardware* assets of Digipoort PI.

Vendor Reckless

a) Vendor recklessness causes a low quality software version to be released into the production environment causing damage to the Digipoort system and renders the system unavailable.
b) Access to servers at the vendor location is not restricted, leading to possible exposure of information.

Employee Disgruntled - Vendors

c) Employee at the vendor purposefully exposes information about the software or hardware.
d) Employee at the vendor purposefully makes the software or hardware unavailable.
e) Employee at the vendor purposefully alters the software code or configuration of the hardware.
f) Employee at the vendor takes away a removable device which contained parts of the software code.

Information assets include not only information flowing through Digipoort PI, but also information about the processes, information about other assets etc related to Digipoort PI. The threat agents like Employee Reckless in Logius, Employee Error in Logius, Employee Disgruntled in Logius, and Internal Spy can cause exposure of information assets. Employees at Logius do not have direct physical access to the infrastructure of Digipoort PI or the information flowing through it. But they have access to information related to the Digipoort PI infrastructure, its vendors, internal processes, and end users/intermediaries.

"*The employees of Logius cannot access the code, but they have insights about the system.....The relevance is not the highest for Logius employees because of the lack of direct access"* says Logius_Expert1 (Interview Set 1 - Appendix IV) about employee threat agent archetypes at Logius. Similarly, an Internal Spy can be more relevant if they are on the vendor side. "*The easiness with which an Internal Spy can access valuable information from Digipoort PI would depend on where the threat agent is; at the vendor side it is easier. At the Logius side it is not very easy but not impossible",* Logius_Expert1 says*.* We created the following sample attack scenarios on the Information assets of Digipoort PI.

Employee Disgruntled - Logius

a) Disgruntled Employee at Logius exposes confidential information regarding vendors/end users/intermediaries of the infrastructure to an external attacker.

b) Disgruntled Employee at Logius takes away key technical documents related to the infrastructure.

Employee Reckless - Logius

c) Reckless Employee at Logius posts 'inside information' about Digipoort PI on a public forum.

Employee Error - Logius

d) An administrator employee at Logius gives privilege on a confidential document to the wrong audience.

Internal Spy

e) An internal spy at Logius shares information regarding vendors/end users/intermediaries of the infrastructure to an external attacker for financial gain.

f) An internal spy at the vendor shares information about the key management system to a hostile agent for financial gain.

g) An internal spy at the vendor shares information about a submitted report to a hostile agent for financial gain.

In the following part we discuss the controls and exposures associated with the sample threat scenarios we discussed above.

Controls and Exposures

The tables 28 to 30 show the minimum controls, existing controls, and possible exposures for the various critical assets of Digipoort PI, based on the sample threat scenarios we developed earlier. The most relevant threat agent for the *Process Infrastructure* asset of Digipoort PI is End User Reckless. From Table 28 we realize that the existing controls can sufficiently mitigate the attack methods due to a reckless end user. Exposure is however possible due to the openness of Digipoort PI for businesses to send information to multiple government agencies using a single valid digital certificate. However its openness and the ease of delivering data to multiple government agencies are also reasons why Digipoort service was implemented by the Dutch government (Bharosa et al., 2015; Logius, 2015r). The controls regarding the validation of messages being sent through various methods, including reporting standards like XBRL and XML, and taxonomies like Netherlands Taxonomy (NT) ensure that the functionalities available to the end users are strictly restricted. This ensures that there are no exposures to Digipoort PI due to end user recklessness.

Table 28: Controls & Exposures for Process Infrastructure Asset

Threat Agent	Examples of Attack Method Description	Minimum Controls Required	Existing Controls	Possible Exposures
End User Reckless	a) Username and password of an end user were compromised as a result of poor security practices at the end user leading to a DDOS attack on Digipoort PI. b) Poor security practices led to theft of digital certificates from the client server which is used by an attacker to send information to DPI.	ISO 27001/27002; BIR; ISO 9001 a) Rules for acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented. b) Users shall only be provided with access to the network and network services that they have been specifically authorized to use. c) Access to information and application system functionalities shall be restricted in accordance with the access control policy. d) Strict rules for authentication and authorization of end users. e) Strong rules for validation of input messages.	Rules for acceptable use a) An interface service specification describes how and under what conditions a connection can be set up between two systems. It contains logistical agreements for the correct addressing, reading, exchanging and processing of messages, as well as agreements for safe and reliable message transmission. Functionality b) Reporting Parties are allowed to send reports according to standards, other functionalities are limited. Standards of reporting like XBRL and XML, and taxonomies like Netherlands Taxonomy (NT), also ensure that proper data structure validation is performed. Authentication/Authorization c) A two-way TLS connection using client and server certificates ensure that reporting and receiving parties are who they claim to be. d) The identity established in the authentication is then used for checking the claimed authorization by checking if there is a valid approval (permission) in a trusted registry. Validation e) During message submission, Digipoort checks the integrity of the message, i.e. the validity of the digital signature. Furthermore, based on the CRL, Digipoort verifies with the CSP that a certificate has not been withdrawn. f) Several checks are included	There are no serious exposures to Digipoort PI due to End User Recklessness. However the fact that Digipoort PI enables users to access multiple Process Infrastructures using a single valid certificate can be a risk to the Process Infrastructures.

Threat Agent	Examples of Attack Method Description	Minimum Controls Required	Existing Controls	Possible Exposures
			in the Supply Service to ensure that messages are secure and any possibility of viruses or DDOS is avoided.	

Table 29 shows the threat agents and the controls and exposures associated with *Information* assets. For a Disgruntled Employee at Logius, exposures could result from the lack of clear guidelines in dealing with a disgruntled employee. Controls like background screening of employees, confidentiality agreements, and training of employees can help in preventing disgruntlement, but controls to deal with attacks due to disgruntlement are not very evident. Similarly there are existing controls that can help mitigate recklessness and prevent errors in the handling of information related assets. However, the use of open standards makes much of the information regarding Digipoort PI publically available. This reduces the risk of exposure due to such threat agents.

Digipoort PI has built in controls for encryption of the information flowing through it, which makes it less motivating for Internal Spies to attack Digipoort PI. Internal Spies at the vendor locations are more relevant as a threat agent due to their direct physical access to the software or hardware infrastructure. However the encryption of information flowing through Digipoort PI using digital certificates and the PKI provides strong controls to ensure the confidentiality of the information flow.

Table 29: Controls & Exposures for Information Assets

Threat Agent	Examples of Attack Method Description	Minimum Controls Required	Existing Controls	Possible Exposures
Employee Disgruntled - Logius	a) Disgruntled Employee at Logius exposes confidential information regarding vendors/end users/intermediaries of the infrastructure to an external attacker. b) Disgruntled Employee at Logius takes away key technical documents related to the infrastructure.	ISO 27001/27002; BIR; ISO 9001 a) Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized modifications or misuse of the information. b) Proper background verification of employees shall be carried out in accordance with relevant laws and regulations. c) Contractual agreements with employees for information security.	Control of separation a) Different departments within Logius are responsible for different parts of Digipoort, reducing the chances for unauthorized modifications or misuse of information. Background checks b) A certificate of good conduct (VOG) is required for every employee before joining Logius. Confidentiality agreements c) Employees are made to enter into confidentiality agreements as part of the contract. Employee trainings d) Training sessions on information security are	We did not find any information regarding the disciplinary process against employees who have committed a breach.

		d) Awareness and training for employees. e) Strong access control policy for the document management system. f) Disciplinary process against employees who have committed a breach. g) Proper definition of duties during termination of employment.	conducted for employees by the information security team. <u>Document Management</u> e) Logius uses the Open Source Enterprise Content Management System by Alfresco to manage the electronic content. <u>Disciplinary process and termination of employees</u> f) No specific information is available regarding this.	
Employee Reckless - Logius	a) Reckless Employee at Logius posts inside information' about Digipoort PI on a public forum.	<u>ISO 27001/27002; BIR; ISO 9001</u> a) Proper Management of physical media to prevent disclosure of information. b) Documented operating procedures should be available for all users. c) Rules for acceptable use of assets are well documented. d) Confidentiality or non-disclosure agreements depending on the type of information being handled. e) Awareness and training for employees. f) Logging and monitoring of events to generate evidence.	<u>Media management</u> a) Media assets are managed according to Logius standards. <u>Information Handling</u> b) Security policy and measures for handling confidential information is documented. <u>Acceptable use of assets</u> c) The Model Code of Conduct for government employees are documented in the 'Modelgedragscode Integriteit sector Rijk' and apply to Logius employees too. <u>Confidentiality agreements</u> d) Employees are made to enter into confidentiality agreements as part of the contract. <u>Employee trainings</u> e) Training sessions on information security are conducted for employees by the information security team. <u>Logging and Monitoring</u> f) Details about logging and monitoring of Logius employees are unavailable.	Information regarding logging and monitoring of employee activities were unavailable. This can lead to recklessness.

Employee Error - Logius	a) An administrator employee gives privilege on a confidential document to the wrong audience.	ISO 27001/27002; BIR; ISO 9001 a) Awareness and training for employees. b) Rules for acceptable use of assets are well documented. c) Strong access control policy for the document management system.	Employee training a) Training sessions on information security are conducted for employees by the information security team. Acceptable use of assets b) The Model Code of Conduct for government employees are documented in the 'Modelgedragscode Integriteit sector Rijk' and apply to Logius employees too. Document Management c) Logius uses the Open Source Enterprise Content Management System by Alfresco to manage the electronic content.	
Internal Spy (Logius/Vendor)	a) An internal spy at Logius shares information regarding vendors/end users/intermediaries of the infrastructure to an external attacker. b) An internal spy at the vendor shares information about the key management system to a hostile agent. c) An internal spy at the vendor shares information about a submitted report to a hostile agent.	ISO 27001/27002; BIR; ISO 9001 a) Encryption of information being transferred through the system. b) Strong access control policy for the document management system. c) Use of confidentiality or non-disclosure agreements.	Encryption 1) Information flowing through Digipoort PI is encrypted using service certificates. The actual information can be seen only by reporting parties and requested parties. Document Management 2) Logius uses the Open Source Enterprise Content Management System by Alfresco to manage the electronic content. Details about the document management at the Vendor are unavailable. Confidentiality agreements 3) Employees at Logius and Vendors are made to enter into confidentiality agreements as part of the contract.	Controls are in place against exposure of information due internal spies.

Vendor Recklessness and Employee Disgruntled at the vendor are the threat agents that are relevant for the *Software and Hardware* assets as shown in Table 30. VENDOR1 and VENDOR2 build and maintain the software and hardware assets of Digipoort PI respectively. Serious exposures with respect to Vendor Recklessness are not present due to the existing controls in the infrastructure. Moreover, both VENDOR1 and VENDOR2 are mandated to follow ISO certifications. VENDOR1 is ISO 9001 and ISO 27001

certified. The datacenters of VENDOR2 are ISO 9001 and ISO 27001 certified. However, lack of documentation on risk management at the vendors makes it difficult to identify the actual controls that are implemented. The lack of visibility on the controls at the vendor is especially clear related to the disgruntled employee threat agent at the vendors.

Table 30: Controls & Exposures for Software & Hardware Assets

Threat Agent	Examples of Attack Method Description	Minimum Controls Required	Existing Controls	Possible Exposures
Vendor Reckless	a) Vendor recklessness causes a low quality software version to be released into the production environment causing damage to the Digipoort system and renders the system unavailable. b) Access to servers at the vendor location is not restricted, leading to possible exposure of information.	ISO 27001/27002; BIR; ISO 9001 a) Separation of development, testing and operational environments. b) Monitoring and review of supplier services. c) Development lifecycle of information systems should be strictly followed. d) Strong access management to server hardware.	Control of separation a) Development, testing and production environments are separated along with strict access control policies. Monitoring of services b) Monitoring and review are performed by the Keteninformatiediensten. ISO certification c) Logius is BIR compliant and therefore follows development lifecycle for information systems. d) Vendors are mandated to be ISO certified and therefore perform suitable access management to the software and hardware assets.	Logius is assuming that the vendor follows all the controls mandated in the ISO standards based on the SLA.
Employee Disgruntled - Vendor	a) Employee at the vendor purposefully exposes information about the software or hardware. b) Employee at the vendor purposefully makes the software or hardware unavailable. c) Employee at the vendor purposefully alters the software code or configuration of the hardware. d) Employee at the vendor takes away a removable device which contained parts of the	ISO 27001/27002; BIR; ISO 9001 a) Screening & Background verification of vendor employees. b) Contractual agreements for information security. c) Restriction on changes to software packages d) Encryption of hardware devices. e) Disciplinary process against employees who have committed a	Background checks a) A certificate of good conduct (VOG) is required for every employee before joining Logius. Confidentiality agreements b) Employees of Vendors and the Vendor organizations are made to enter into confidentiality agreements as part of the contract. Change management c) Changes to software are restricted based on strict policies.	Logius does not have clear information regarding the security controls in the infrastructure like whether the hardware is encrypted or not. There is also no information regarding the disciplinary actions against disgruntled vendor employees.

Threat Agent	Examples of Attack Method Description	Minimum Controls Required	Existing Controls	Possible Exposures
	software code.	breach. f) Awareness and training for employees. g) Proper definition of duties during termination of employment h) Proper logging and monitoring of employee activities	Encryption of hardware d) No documented information is available. Disciplinary process e) No documented information is available. Employee trainings at vendors f) VENDOR1 conducts risk awareness sessions for its employees. Termination of employment g) All the accesses and permissions of employees terminating their services are revoked and administrator accounts if any are deleted. Logging & Monitoring h) Employee activities in the servers and databases are monitored and logged.	

Threat Landscape - Digipoort PI

The following threat agents were found to be prominent in the threat landscape of Digipoort PI. Reckless actions of End Users were found to be relevant for the *Process Infrastructure* asset of Digipoort PI. There were no serious exposures found with respect to this threat agent for the sample attack scenarios we considered. The openness of Digipoort PI can lead to the reckless use of the infrastructure. Anyone who has a valid PKIOverheid certificate can submit a message to Digipoort PI. However, traceability based on the certificate holder's registration and the logs of activities (also known as the audit trail) ensures that recklessness is noticeable (Bharosa et al., 2015). We know from the TAL (Figure 23) that reckless end users do not have a malicious intention to attack. The possibility of a Man-In-The-Middle (MITM) attack, capitalizing on the recklessness of an end user however cannot be ignored. The End Users should have their own internal security measures and security policies in place. Generic IT security mechanisms such as firewalls and intrusion detection must be up and running. The End Users themselves have a paramount role in maintaining sufficient information security (Bharosa et al., 2015)

The threat landscape of Digipoort PI also has many insider threat agents. According to the definition of 'Insider Threats' given by Humphreys (2008), Employee Disgruntled, Employee Reckless, Employee Error, Internal Spy, and Vendor Recklessness can all be considered under the category of 'Insider Threats'. Of

these, disgruntlement, recklessness, errors, or spying by the Logius employees might not lead to the exposure of information flowing through Digipoort PI due to the lack of direct physical access to the infrastructure. It can however lead to exposure of information related to Digipoort PI or its assets. The risk of exposure is however low due to the use of open standards in the implementation of Digipoort PI, which makes most of the information publically available.

Vendors of Digipoort PI have direct physical access to the software and hardware assets of the Digipoort PI infrastructure. For this very reason, the relevance of threat agents like Employee Disgruntled, Internal Spy and Recklessness at the vendors is high. Employee disgruntlement can lead to high exposures and is a very important threat agent in the threat landscape of Digipoort PI. There might be existing controls to mitigate the actions of a disgruntled vendor employee, but they are obscure. This raises the possibility of an exposure due to this threat agent. Controls implemented to mitigate attacks due to Vendor Recklessness seemed sufficient for the sample attack scenarios we proposed. Risk of exposure due to Internal Spies at the vendors is also higher than internal spies at Logius, because of their possible direct physical access to hardware or software assets. Logius can benefit from having a clearer visibility on the activities of the vendors, in the form of better documentation of vendor activities. Maintaining consolidated risk assessment documentation on Digipoort PI at Logius will make it easier to identify clearly the existing controls related to these threat agents.

Even though internal vendors were lower in priority as a threat agent compared to the external vendors of Digipoort PI infrastructure, they are important from a risk assessment perspective. Contract management with internal vendors is as important as the contract management with external vendors. This is something that can be taken into account during a risk assessment of Logius. Further discussion on this topic is beyond the scope of this report. We have limited ourselves to only a peripheral analysis of the various assets of Digipoort PI here due to the constraints of this research. In actuality, each of the assets can be comprehensively evaluated in the way we applied the methodology to the Key Management asset in Chapter 6. Performing such an analysis will certainly help Logius in creating a very comprehensive threat landscape for Digipoort PI.