The After-effects of the DigiNotar Crisis: A Closer Look

Changes in Public-Private Partnerships in the PKIoverheid System in Response to the DigiNotar Crisis

Master's Thesis
Final version - 07-06-2018
Crisis and Security Management
by Redmar Jager - S1984152
25.217 words

Universiteit Leiden
Governance and Global Affairs

Supervisor: Dr. J. Reijling
Second reader: Dr. E. de Busser

Index

1. Introduction

This chapter first introduces the subject of this thesis and provides the context necessary to understand the thesis' significance. It will then present the research question and will continue by discussing the academic and societal relevance of this study. A short reading guide to explain the structure of this thesis will finalize this chapter.

1.1 Context

In 2011 the Dutch certificate authority DigiNotar was hacked. DigiNotar started its business by issuing digital certificates that had to secure confidential internet communication between public and private parties, in particular civil-law notaries and government agencies. Gradually, DigiNotar expanded its business and became a certificate authority in the PKIoverheid system, a public key infrastructure run by the Dutch government. Public key infrastructure (PKI) is the entire system of components that manages the issuance, storage, and distribution of digital certificates. Security and trust are paramount in successfully running a PKI (Maurer, 1996: p. 325-326).

Whilst DigiNotar was hacked, the intruder managed to falsify 531 digital certificates for a wide range of websites, varying from the domains of Microsoft to the domains of the Mossad (Fox-IT, 2012: p. 59). Using false certificates, the hacker intended to place himself between two parties to intercept or alter confidential information, a man-in-the-middle attack (Fox-IT, 2012: p. 6). The hacker had chosen DigiNotar, because it had a good reputation and was on the trust lists of many well-known operating systems and web browsers (Fox-IT, 2012: p. 59).

After a rogue DigiNotar certificate was discovered by an Iranian Gmail-user, the Dutch Ministry of Interior and Kingdom Relations hired the private Dutch information security company Fox-IT to investigate the situation. Fox-IT subsequently reported that a large amount of Iranian citizens was targeted through that same rogue certificate that was fabricated by the hacker of DigiNotar (Fox-IT, 2012: p. 6).

Quickly, the DigiNotar crisis made international headlines and, as a result, its digital certificates were labeled untrustworthy and had to be revoked. As the server that had stored the PKIoverheid certificates was compromised as well, the Dutch PKIoverheid system suffered from an erosion of trust too. Its stakeholders had to put in major efforts to guarantee the continuity of government services that made use of DigiNotar's PKIoverheid certificates. In the meanwhile, DigiNotar saw its reputation damaged so severely, that it soon had to file

for bankruptcy. DigiNotar since then is regarded as a major Dutch digital disaster (Van der Meulen, 2013: p. 46).

After the crisis was resolved, an official government inquiry by the Dutch Safety Board (OVV) followed. The inquiry report exposed negligence on the part of DigiNotar, but also lack of oversight by the Dutch government. The inquiry report stated that the public-private partnership between both parties had fared too much on trust and too little on regular audits and adequate oversight (OVV, 2012: pp. 48-49). The OVV concluded that the oversight arrangements of the PKIoverheid system were irresponsible (OVV, 2012: p. 42), and made recommendations for the safer issuance of digital certificates, but also for Dutch cyber security policy as a whole (OVV, 2012: pp. 86-87).

The recommendations for the safer issuance of digital certificates mainly concerned a change in the oversight arrangement between Logius, OPTA, and the certificate authorities. Logius was the government organization that managed the PKIoverheid system, and OPTA was the Dutch telecom watchdog that was responsible for oversight on organizations that issued qualified certificates (OVV, 2012: p. 87). OPTA was partly responsible for oversight on DigiNotar, as DigiNotar was entitled to provide qualified certificates, which also could be issued in the PKIoverheid system.

Furthermore, OVV recommended to promote cultural change among certificate authorities, in particular with regard to reporting security incidents and how to learn from such incidents (OVV, 2012: p. 87). These recommendations were heeded by the Dutch parliament, as suggested by the official response on the OVV's recommendations by Dutch Minister of Interior and Kingdom Relations, Ronald Plasterk. Plasterk called the DigiNotar crisis a "wake-up call" and announced "extra commitment" to make the Netherlands' digital infrastructure more secure (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties [MinBZK], 2012d: p. 1).

This study seeks to establish if the DigiNotar crisis indeed led to a change in the characteristics of the PKIoverheid system and, if so, to what extent these changes can prevent new security breaches. The study will mainly use theory on networks by Whelan (2011) to analyze the characteristics of public-private partnerships before and after the DigiNotar crisis. The thesis uses theory on networks, as the Dutch national cyber security strategies speak of public-private partnerships as structures or networks (NCTV, 2013: p. 8).

1.2 Research question

This study aims to research if and how the DigiNotar crisis changed the characteristics of public-private partnerships in the PKIoverheid system, and to see if lessons truly were learned. This leads to the following research question:

To what extent has the DigiNotar crisis changed the characteristics of public-private partnerships in the PKIoverheid system, and how can this be explained?

1.3 Academic relevance

The DigiNotar crisis was a major digital crisis, because it involved the large-scale issuance of false digital certificates and the compromise of the government accredited PKIoverheid certificates. Digital certificates are a key ingredient for secure internet traffic and therefore one of the cornerstones of the internet's infrastructure. Although one would expect that a crisis with such important certificates would have led to extensive academic study or debate, the DigiNotar crisis and its consequences still remain relatively understudied and rendered only a limited amount of academic literature. This study aims to fill that gap.

Furthermore, this study intends to add to the current body of knowledge by applying existing literature on networks by Whelan (2011), Provan and Kenis (2008), and Kenis and Provan (2009) to public-private partnerships in the Dutch cyber security landscape. By using this literature, the study tries to establish if theory on networks can also be used to analyze public-private partnerships, which often resemble network structures. Studying possible change in the characteristics of public-private partnerships in the cyber domain will also add to the broader academic debate on the consequences of delegating government activities to the market.

1.4 Societal relevance

Public-private partnerships have for long been playing an important role in the provision of information technology services and in building cyber resilience, since a lack of capacity and a lack of expertise have been limiting the state's ability to provide for these services. The private sector has stepped in to offer cyber security services to the government, to the public, and to anyone else who is willing to pay for it. Changing roles and responsibilities in the provision of information technology and cyber security thus seem necessary, but these changes often come at a cost due to a conflict of interest.

The study finds its societal relevance by studying these changing roles and responsibilities of both the public and the private sector in their provision of vital components – digital certificates - for secure and trustful use of the internet by its citizens, its businesses, and the government itself. However, public-private partnerships on cyber security matters raise questions about accountability, legal mandate, and privacy. For instance, does accountability for potential mistakes or failures lie with the public or with the private sector? Under what legal mandates do public and private actors operate to achieve their goals? And how is data protection guaranteed, especially now the General Data Protection Regulation (GDPR) has come into force?

Studying change of characteristics of public-private partnerships in the PKIoverheid system fits in that broader debate on the changes in the provision of security and contributes to gaining valuable knowledge on the potential consequences of these changes. Expanding knowledge on this topic will for long remain relevant, now digitalization has become so pervasive in daily life that cyber security - or a lack thereof - has the potential to impact nearly all layers of contemporary society, whether it concerns the public, the private, the collective, or the individual.

1.5 Reading guide

This introduction has shed light on the context, relevance, and the focus of this thesis. In the second chapter, the theoretical framework is set out and will combine elements of different academic disciplines to provide more details about the main themes of this thesis: public-private partnerships, network dynamics, and cyber security. In chapter 3, the methodology of this study is explained. The methodology will bring structure to this thesis and will give insight in the choices that were made to fulfill this study.

Chapter 4 first answers the study's sub questions and will shed more light on the workings of digital certificates, on the DigiNotar crisis, and on how public-private partnerships in the PKIoverheid system can be described. Chapter 4 is finalized with an answer to the main research question. In chapter 5, a reflection on this thesis is presented, in which will be elaborated on the academic and societal relevance of this study, leading to recommendations for policy and further study. Lastly, the bibliography lists the written sources that were used for this study. The interview protocol and relevant transcripts from the interviews can be found in the appendices.

2. Theoretical framework

In this chapter, the theoretical framework is set out. The theoretical framework first introduces existing literature to come to a general definition of public-private partnerships. Secondly, it discusses theory on the characteristics of networks. Lastly, the theoretical framework links public-private partnerships to the field of cyber security. This theoretical framework will conclude with an analytical framework, which can be used as a model to study the characteristics of public-private partnerships.

2.1 Public-private partnerships

The concept of public-private partnership suggests that it is a partnership in which public and private parties work together to provide for a certain product or service. Klijn & Teisman (2003) use a similar definition, but stress the basic premise of mutual benefit. They have defined a public-private partnership as a "cooperation between public and private actors with a durable character in which actors develop mutual products and/or services and in which risk, costs, and benefits are shared" (p. 137). Benefits can vary from financial to reputational and can differ per side of the partnership.

As Wettenhall (2003: p. 77) rightly noticed, public-private partnerships come in many forms and cover many things. Above all, public-private partnership also has been a fashionable word. Wettenhall (2003: p. 80) illustrates the contrapositions on public-private partnerships by observing how proponents of New Public Management believe how a public-private partnership is a market-serving economic technique not particularly meant to serve the public interest, whilst proponents of governance believe that public-private partnerships do recognize the public interest and can balance market mechanisms.

Linder (1999: p. 42) also recognized that different perspectives on public-private partnerships have proliferated. He identified six frequent, but distinctive uses of the concept: public-private partnership as (1) management reform, as (2) problem conversion, as (3) moral regeneration, as (4) risk shifting, as (5) restructuring public service, and as (6) power sharing. Without explaining each perspective, we already see substantial differences in the interpretation of public-private partnerships. Linder (1999: p. 49) also notes that the nature of public-private partnering can vary from financial aid in form of subsidies to the outsourcing of public services to the private sector, adding even more layers to the concept.

This study will use Klijn and Teisman's (2013) definition of public-private partnership, because of their acknowledgement that risks, costs, and benefits are shared. Furthermore, the study will built on Linder's broad perception on types of public-private partnerships, as the specific arrangements of the PKIoverheid system first require more study before singling out certain types of partnerships. Now, the next section will go deeper into the levels of analysis that will be used to study public-private partnerships.

2.1.1 Public-private partnerships as networks

To study the characteristics of public-private partnerships, the public-private partnership's administrative structure requires more explanation. In this study, public-private partnerships are studied as networks, as such partnerships consist of at least two parties that are interdependent, but operate autonomously within a relatively institutionalized framework, contributing to the production of public purpose (Sørensen and Torfing, 2005: p. 197).

This section introduces frameworks by Provan and Kenis (2008), Kenis and Provan (2009), and Whelan (2011) that were developed to study the performance and the effectiveness of networks. These frameworks outline components of networks that are relevant for achieving the network goals for different types of networks, and help to come to a better shared situational awareness, in which the participants in the network have a common operational picture about a certain situation (Kurapati, Kolfschoten, Verbraeck, Drachsler, Specht & Brazier, 2012: p. 48).

The study will use the parameters as discussed in these frameworks to study a possible change in the characteristics of public-private partnerships after the DigiNotar crisis was resolved. The next section will first address the works of Provan and Kenis (2008) and Kenis and Provan (2009). Second, it will the introduce the framework that was developed by Whelan (2011).

2.1.2 Network governance and performance

With Provan and Kenis (2008) earlier having introduced a taxonomy of three different types of network governance models, Kenis and Provan (2009) elaborated on the performance of each type of network governance models by pointing out each model's strengths and weaknesses, and by discussing how each type of network governance suits a certain group of organizations best. Kenis and Provan (2009) hereby stressed the need for appropriate performance criteria for each type of network governance model. This section discusses these three types of network governance model and the characteristics that come with it.

2.1.2.1 Shared or participant-governed network

The shared or participant-governed network is characterized by the participants' equality in power and in participation. There is no formal lead agency, instead the network is decentralized and proceeds collectively to attain its goals. The size of a shared or participant-governed network often is small, which benefits active involvement by all parties (Provan & Kenis, 2008: pp. 234-235).

Information flows directly between the network participants. However, because the participant-governed network is oriented towards collective action and consensus among all members, this type of network is also bound to be ineffective. A lack of consensus can negatively influence the participants' commitment to the network goals. It works best for smaller networks with high interactivity, often at local level (Kenis & Provan, 2009: p. 446).

2.1.2.2 Lead organization-governed network

In the lead organization-governed network, power is much more centralized. One key organization holds asymmetrical power over the other members of the network. The lead organization facilitates and decides on the network's undertakings towards the network goals, which often are in line with the lead organization's goals (Provan & Kenis, 2008: p. 235).

The lead organization provides legitimacy and is key to efficient decision-making, hereby suiting a large amount of network members. Yet, regarding goal consensus, the lead organization may push its own agenda, frustrating other network members. In due time, this can lead to other network members pursuing non-network interests, affecting the overall performance of the whole network (Kenis & Provan, 2009: pp. 447-448).

2.1.2.3 Network administrative organization model

In a network administrative organization model, a separate administrative organization functions as the network facilitator. This network administrative organization is exclusively occupied with governing the network and often consists of only few board or staff members (Provan & Kenis, 2008: p. 236).

A network administrative organization is usually set up when a network is still in an early stage of development. The network administrative organization can smoothen the development of the network and can guide the network to its goals. Sustainability and legitimacy are the core strengths of the network administrative organization model, whilst

overreliance on the network administrative organization by its participants can be a weakness (Kenis & Provan, 2009: p. 448).

2.1.2.4 Network performance

Kenis and Provan (2009: p. 449) argued that each type of network governance model has different core attributes and requires different performance criteria. Next to type of network governance model, it is also important to look at whether a network has been set up voluntarily or whether a network has been mandated. This can affect the legitimacy within the network, but also the legitimacy of the network to the outside. The willingness to go beyond one's own organization to further the goals of the network will also be strongly dependent on how the network was set up (Kenis & Provan, 2009: 440-450).

Kenis and Provan (2009: p. 451) also proposed that the stage of development of a network calls for appropriate performance criteria, as a young network first needs to develop itself before it becomes as efficient as more mature networks.

With the ideas of Provan and Kenis (2008) and Kenis and Provan (2009) in mind, the next section will look into Whelan's (2011) framework on network dynamics and network effectiveness. Whelan's (2011) clearly has taken notice of the works of Provan and Kenis (2008) and Kenis and Provan (2009), and elaborates further on it.

2.1.3 Network dynamics and effectiveness

Whelan (2011) developed a methodological framework for networks in the domain of national security to advance the knowledge of such networks, in particular the knowledge on network dynamics and network effectiveness. This thesis will use Whelan's (2011) framework as the basis for analysis, as digital certificate services have an important place in the cyber security landscape, which in turn has become a critical component of national security.

Similar to Sørensen and Torfing (2005), Whelan (2011) argued that a network "involves repetitive exchanges between a set of autonomous but interdependent organizations in order to achieve individual and shared objectives" (pp. 276-277). Networks differ from hierarchy or market forms of governance, because they are controlled through relationships that are based on trust and reciprocity instead of administrative means or economic incentives (Whelan, 2011: p. 277).

Whelan (2011) proposed a methodological framework that constitutes of five interdependent levels of analysis. Central to the dynamics of networks are the (1) network structure and the (2) network relationships. To better understand how this relates to the effectiveness of the network, Whelan (2011) complemented his framework with the features (3) network culture, (4) network policies, and (5) network technologies. The following paragraphs will discuss each level of analysis individually.

2.1.3.1 Network structure

Network structure refers to the design and the size of the network, but also to the role of the organizations within the network. Whelan (2011: pp. 278-279) identified two basic designs: (1) the hub and (2) the all-channel network. These structures relate to the flow of information and to who has control over the network. In a hub, the network is led by one actor that controls the flow of information. In the all-channel network, all actors are organically connected to each other and no single actor holds central control (Whelan, 2011: p. 279).

The hub network is thus similar to Provan and Kenis' (2008) lead-organization governed network, and the all-channel network resembles the shared or participant-governed network. Internal network governance of the hub network is brokered, for an all-channel network it is shared. Whelan (2011: p. 279) argued that no form of governance is preferable over another. Instead, he suggests a dynamic process of structuring and restructuring to respond to contingencies or to adopt new actors. Shared or brokered governance depends on the size of the network and the need for a coordinating actor.

2.1.3.2 Network culture

Whelan (2011: p. 280) defined culture as shared beliefs, values, and attitudes. He distinguishes culture of networks at two levels: (1) the singular network culture, referring to the shared culture of the network as a whole, and (2) the plural network cultures, referring to the different cultures pertaining to the individual organizations in the network. Both forms of culture can have implications for the network's effectiveness.

Network culture is more than the accumulation of all different cultures of the network members. It is the own culture of the network as a whole, often developed after a considerable period of time, solid membership, and shared emotional experiences (Whelan, 2011: p. 280). Network cultures, on the other hand, are the different cultures of the network members. Cultural differences are important to recognize. If these differences are not

managed properly, this can have negative consequences for the network effectiveness (Whelan, 2011: p. 280).

2.1.3.3 Network policies

Whelan (2011: pp. 280-281) stated that network policies relate to internal network control and to the policies and procedures to enhance this control. Regarding security, this refers largely to arrangements about information sharing and the division of roles and responsibilities in the network. Network policies are connected to network culture, because policy can enforce cultural changes, but policy also needs to be supported by culture to be effective.

Network policies also implicate a trade-off between flexibility and stability. Policies enhance network stability, but curtail the flexibility of the network. Stability is essential for networks that are engaged in long-term projects in order for network members to develop relationships and for establishing a steady delivery of services. However, stability also means that the network can be inflexible when it has to adapt to change efficient (Whelan, 2011: p. 281). Whelan (2011: p. 281) pointed out that a network needs a clear policy framework, but preferably as minimalist as possible. Policy has to be under constant review in order for the network to remain flexible and efficient.

2.1.3.4 Network technologies

Network technologies comprise the technological infrastructure of a network. Organizational networks are often built around information exchange and use information and communication technologies to do so. As this information exchange tends to be intensive, the technological infrastructure needs to be designed to exchange this information efficiently and effectively. However, the technological infrastructure does need to support the network goals to really benefit the network performance (Whelan, 2011: p. 281).

Problems than can arise when the technological infrastructure does not fit the network are limited interoperability and information overload, both common phenomena in the field of national security. Such problems can be tackled by developing clear network policies, which determine the access to technological systems and the relevance of information per agency (Whelan, 2011: pp. 281-282). Proper use of network technologies is believed to benefit the shared situational awareness of the network, which in turn benefits the network effectiveness (Boersma, Wagenaar & Wolbers, 2012: p. 3).

2.1.3.5 Network relationships

Network relationships relate to the formal and informal relationships between organizations, its employees, and other units within the network. Network relationships are essential to network effectiveness (Whelan, 2011: p. 278). According to Whelan (2011: p. 282), trust is crucial in these relationships. Whelan (2011: p. 282) argued that trust exists when there is risk and when there is interdependence. More risk or more interdependence generally means that trust is more important for the network to function properly. This can be trust in natural persons, but also trust in the partner organization.

Whelan (2011: p. 282) posited that network relationships are possibly the most important level of analysis. He argued that when trust is high, it is more likely that problems that are related to network structure, culture, policies, and technologies will be overcome. Furthermore, network effectiveness is expected to be higher when interpersonal relationships are strong. Such relationships can be applied to use informal contacts to solve or overcome formal problems. Whelan (2011: pp. 282-283) points out that using informal contacts can lead to problems as well, but this is for the network manager to keep an eye on.

2.2 Public-private partnerships and cyber security

Now public-private partnerships and network characteristics have been discussed, it is necessary to couple this to the field of cyber security, which digital certificate services are part of. Although public-private partnerships were by no means new during the development of the internet's infrastructure in the 1980s, it was the Clinton-led administration that really pushed the private sector to invest in the internet in the early 1990s (Carr, 2016: pp. 47-48). Therefore, public-private partnerships can be considered a traditional component of the internet and thus an important feature of cyber security. To better understand the meaning of the concept cyber security, this section provides a definition.

In a comparative study of national cyber security strategies Luijff, Besseling and De Graaf (2013) pointed out the variety of definitions of cyber security that nineteen different countries use in their national cyber security strategy. Whereas the Netherlands, defines cyber security briefly as "to be free from danger or damage due to the disruption or destruction of ICT, or due to the abuse of ICT" (Luijff *et al.,* 2013*:* p. 6), France defines cyber security more broadly as "an information system allowing to resist likely events resulting from cyber space which may compromise the availability, the integrity or confidentiality of data stored, processed or transmitted and of the related services that information and communication (ICT) systems offer" (Luijff *et al.,* 2013*:* p. 6).

When reading all nineteen definitions in the study of Luijff *et al.* (2013), it becomes clear that cyber security has many referent objects: critical infrastructure, the economy, the military, but also personal integrity. It is often only the technology that connects these referent objects, says Carr (2016: p. 50). Dunn Cavelty (2014: p. 4) rightly noticed that, although an important element, personal integrity frequently does not feature in the policy discourse, in which privacy, anonymity, and freedom of speech are only seldom mentioned.

This study sees particular use in Carr's (2016) definition of cyber security, as it incorporates referent objects that are closely linked to digital certificate services. Carr (2016) stated that cyber security refers to "the integrity of our personal privacy online, to the security of our critical infrastructure, to electronic commerce, to military threats and to the protection of intellectual property" (pp. 49-50). Digital certificate services reach the core of online integrity, can be seen as critical internet infrastructure, and play an important role in securing trust in electronic commerce.

Furthermore, this thesis is particularly interested in culture towards security and risk in the field of cyber security and will analyze this by using elements of Jahner and Krcmar's (2005) framework on information technology risk culture, of which the development was

motivated by an increasing amount of cyber security incidents. In this framework, Jahner and Krcmar (2005: p. 3330) argued that risk culture is based on the way risks are identified and acknowledged as threats, the way risks are communicated forthright throughout the organization, and the way an organization acts to mitigate and control risks and threats.

For the identification and acknowledgment of risks, Jahner and Krcmar (2005: p. 3331) posed that management and employees have to recognize that the organization is exposed to risk simply by using information technology. Jahner and Krcmar (2005: p. 3331) understood that this sounds trivial, but stated that management often assumes that high technical security standards and well-developed processes diminish risk. Yet, such an assumption is deemed delusive and leads to inefficient security measures.

The communication of risks throughout the organization is a key element of risk culture, because it creates a shared understanding of threat among management and employees. The communication of risk throughout the organization also encourages integer behavior by employees, creates risk awareness, and generates trust (Jahner & Krcmar, 2005: p. 3331).

Lastly, Jahner and Krcmar (2005: p. 3331) stressed that, as soon as risk is identified, acting accordingly is paramount. This can be the implementation of measures that intensify technical security, but this can also be organizational measures that instruct employees about security awareness and behavior codes. With regard to technical security measures, Jahner and Krcmar (2005: p. 3331) specifically mentioned that these apply to public key infrastructures, the field in which the PKIoverheid system operates.

2.3 Analytical framework

The theory and literature discussed in the previous sections will be used to define an analytical framework to study the characteristics of public-private partnerships in the PKIoverheid system before, during, and after the DigiNotar crisis. The study's sub questions are composed in accordance with this framework.

2.3.1 Analytical model

Whelan's (2011) framework to analyze network dynamics and effectiveness is the basis for the analytical model. Therefore, the five levels of analysis are (1) network structure, (2) network culture, (3) network policies, (4) network technologies, and (5) network relationships. Additionally, the framework will incorporate ideas from Provan and Kenis (2008) and Kenis and Provan (2009) to study network structure. To study culture, the ideas of Jahner and Krcmar (2005) on risk culture in information technology environments are also implemented in the model.

Together, this leads to an analytical framework that is the basis for study and shows the study's main themes:

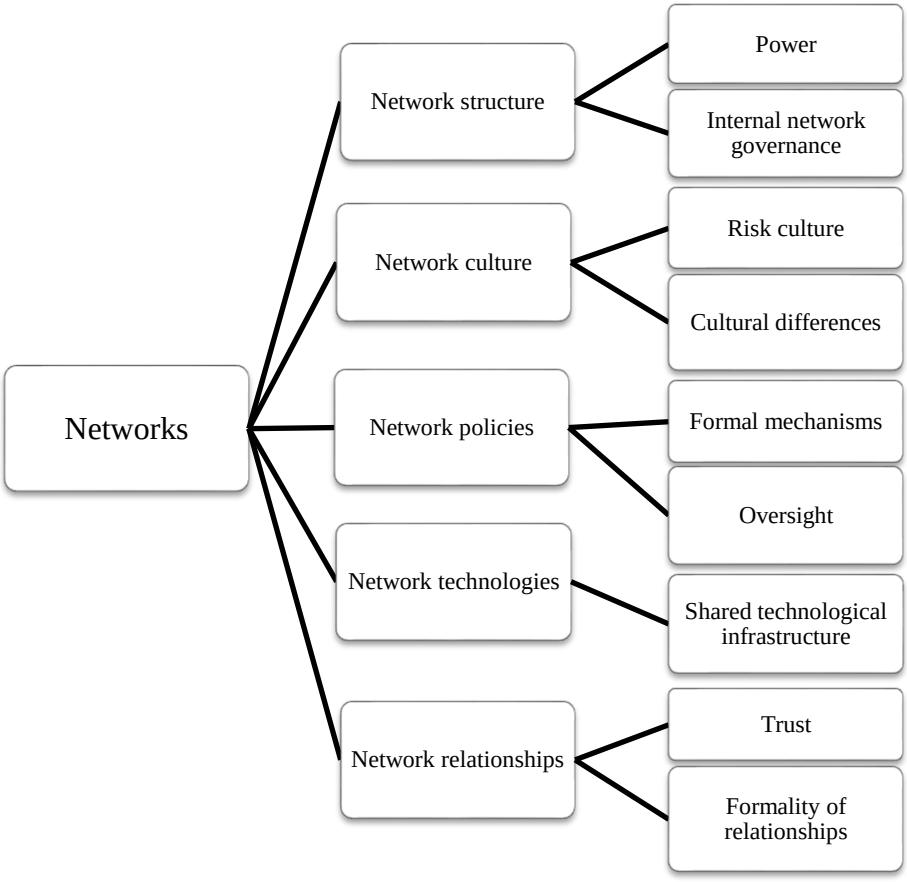

Figure 1: Analytical framework.

The study will mainly use this model to study possible changes in the characteristics of networks, but in due time the network effectiveness will come to the fore as well. The levels of analysis are further operationalized in chapter 3.3.2.

2.3.2 Sub questions

The previously developed analytical model will be used to answer the following sub questions, which will provide the study with a general structure and will serve as a guide for answering the main research question.

1. What was the DigiNotar crisis?

Answering this question will lead to a description of DigiNotar, digital certificates in general, the PKIoverheid system, the DigiNotar crisis, and the context in which it happened. The answer to this sub question contributes to a better understanding of possible changes in the characteristics of public-private partnerships in the PKIoverheid system.

2. What were the characteristics of public-private partnerships in the PKIoverheid system before the DigiNotar crisis, and how does this relate to the events of the DigiNotar crisis?

Answering this question will lead to an analysis of the characteristics of public-private partnerships in the PKIoverheid system before the DigiNotar crisis, and how these characteristics relate to the DigiNotar crisis. The analysis uses the analytical framework that was based on Provan and Kenis' (2008) and Kenis and Provan's (2009) theories on network governance, Whelan's (2011) framework on network effectiveness, and Jahner and Krcmar's (2005) ideas about risk culture.

3. What are the characteristics of public-private partnerships in the PKIoverheid system after the DigiNotar crisis, and how does this relate to the events of the DigiNotar crisis?

Answering this question will lead to an analysis of the characteristics of public-private partnerships in the PKIoverheid system after the DigiNotar crisis, and how these characteristics relate to the DigiNotar crisis. The analysis uses the analytical framework that was based on Provan and Kenis' (2008) and Kenis and Provan's (2009) theories on network

governance, Whelan's (2011) framework on network effectiveness, and Jahner and Krcmar's (2005) ideas about risk culture.

After these sub questions have been answered, the main research question will be answered in the conclusion, which will compare the characteristics of public-private partnerships in the PKIoverheid system before and after the DigiNotar crisis. This conclusion will also try to explain for similarities and differences in these characteristics and to what extent these relate to the DigiNotar crisis.

Lastly, a reflection on the research will take place, which will look into recommendations for policy or into avenues for further study.

3. Methodology

This segment introduces the research methods that will be used in this study. The chapter will address and justify the chosen research design, the methods for data collection, the methods for data analysis, and the study's validity. Setting out the study's methodology provides a structured way of working and makes the study verifiable and replicable.

3.1 Research design

The study is a comparative analysis of the changes in the characteristics of public-private partnerships in the PKIoverheid system in response to the DigiNotar crisis. The study will use qualitative methods to analyze the organizational context in which the DigiNotar crisis took place, and to analyze and to explain for the changes in the characteristics of public-private partnerships in the PKIoverheid system in response to the DigiNotar crisis. A comparative design fits this study best, as it wants to study the characteristics of public-private partnerships in the PKIoverheid system in a before-and-after fashion.

The DigiNotar crisis is chosen as the central event, as it is widely seen as a wake-up call for securing the internet's infrastructure (MinBZK, 2012d: p. 1; Van der Meulen, 2013: p. 55; Wolff, 2016). As the crisis escalated through failing public-private arrangements (OVV, 2012: pp. 48-49), the characteristics of public-private partnerships in the PKIoverheid system will be the focus of this study.

3.2 Data collection

The study will mainly use document analysis to construct a rich image of the DigiNotar crisis and the context in which it took place. The study will use publicly accessible government records (e.g., official strategies, reports, and letters to the House of Representatives), independent inquiry reports, media reports, and complementary academic literature to describe the DigiNotar crisis and to map the public-private partnerships in the PKIoverheid system.

Next to document analysis, the study will seek to interview relevant stakeholders from the PKIoverheid system and the Dutch cyber security sector to triangulate the results from the document analysis and to break new ground. Semi-structured interviews with important stakeholders and experts are expected to shed more light on differences between written truth and perceived truth. To validate this perspective on the topic, this study has conducted seven interviews.

Among the interviewees are a senior official at the Ministry of Interior and Kingdom Relations, which is the commissioning ministry for the PKIoverheid system; the Policy Authority for PKIoverheid at Logius, which is the administrator of the PKIoverheid system; a senior coordinating advisor at the NCSC, which coordinates and facilitates public-private partnerships in the Dutch cyber security sector; a senior coordinator at Agentschap Telecom, which is the current oversight authority on telecom-related services and products; and three stakeholders from private organizations that issue PKIoverheid certificates Digidentity, QuoVadis and KPN. All interviewees have witnessed the DigiNotar crisis or its aftermath from close-by.

The variety in the backgrounds of the interviewees should generate a balanced account of changes in public-private partnerships in the PKIoverheid system in response to the DigiNotar crisis. The list of names of the interviewees and the interview protocol can be found in Appendix I. The relevant extracts of the interviews can be found in Appendix II.

3.3 Data analysis

This section discusses the data analysis and the operationalization of the analytical model that was developed in chapter 2.3.1.

3.3.1 Methods

The document analysis builds on the basics of qualitative content analysis. The documents are collected from government and relevant organizations' websites and were studied for themes that are part of the analytical framework. The process of identifying themes that are of interest to this study is not specified in detail, but relevant parts are illustrated with quotations or references to the source (Bryman, 2012: p. 557).

The interviews have been recorded digitally and have been transcribed. After transcribing the interviews, themes from the analytical framework have been identified by using a coding scheme. After coding the interviews, quotes from the interviews have been used to make or to support observations. Relevant parts of the transcription can be found in Appendix II.

3.3.2 Operationalization

To analyze the data, the study's theory has to be operationalized. Based on the analytical framework, the operationalization scheme lists the indicators that the study wants to measure. The operationalization chart on page 22 shows the five components of Whelan's (2011)

literature on networks, and the more specific ideas of Provan and Kenis (2008), Kenis and Provan (2009), and Jahner and Krcmar (2015).

Network structure is measured in power, which is divided in the indicators lead role and consensus, based on the taxonomy of network models by Provan and Kenis (2008); and in internal governance, of which the indicator is the control over information flows. This refers to the hub and the all-channel designs by Whelan (2011), and the brokered or shared governance by Provan and Kenis (2008).

Network culture is measured in attitudes and beliefs with regard to risk culture, which is divided in the indicators security attention and risk awareness, based on the work of Jahner and Krcmar (2005); and in cultural differences, which is indicated by the degree of heterogeneity of the same attitudes and beliefs. This is based on Whelan's (2011) idea that cultural differences can affect the network effectiveness.

Network policies, which Whelan (2011) described as the formal policies and procedures for network control, are measured in three levels of regulation that are expected to have most impact on the PKIoverheid system: official legislation, network specific requirements, and industry self-regulation. Compliance with the regulation for internal network control then is measured by oversight, which is indicated by audits and company visits. These specific indicators are chosen because of the negative role of oversight arrangements before the DigiNotar crisis and are partly deducted from the recommendations by OVV (2012).

Network technologies are measured by analysing the shared technological infrastructure that is used to exchange information in order to enhance network effectiveness, as proposed in Whelan's (2011) framework. The study will mainly look at communication technology and possible use of shared databases in which, for example, certificates are registered.

Network organizations will be measured in trust, which is divided in interpersonal trust and interorganizational trust. This is derived directly from Whelan's (2011) framework. The study will also seek to measure the formality of relationships in the network. According to Whelan's (2011) framework, formal and informal procedures or contacts can affect the network effectiveness and can help overcoming problems. The indicators are formal procedures and use of informal relationships.

Together, these indicators form the operationalization scheme. The operationalization scheme is the guideline for structuring the data that comes forth out of the document analysis and the interviews. After gathering and analysing the data, the ultimate test will be to see if

the network characteristics are beneficial to the network goals and to what extent this contributes to the shared situational awareness among the network participants. The following chart displays the operationalization scheme:

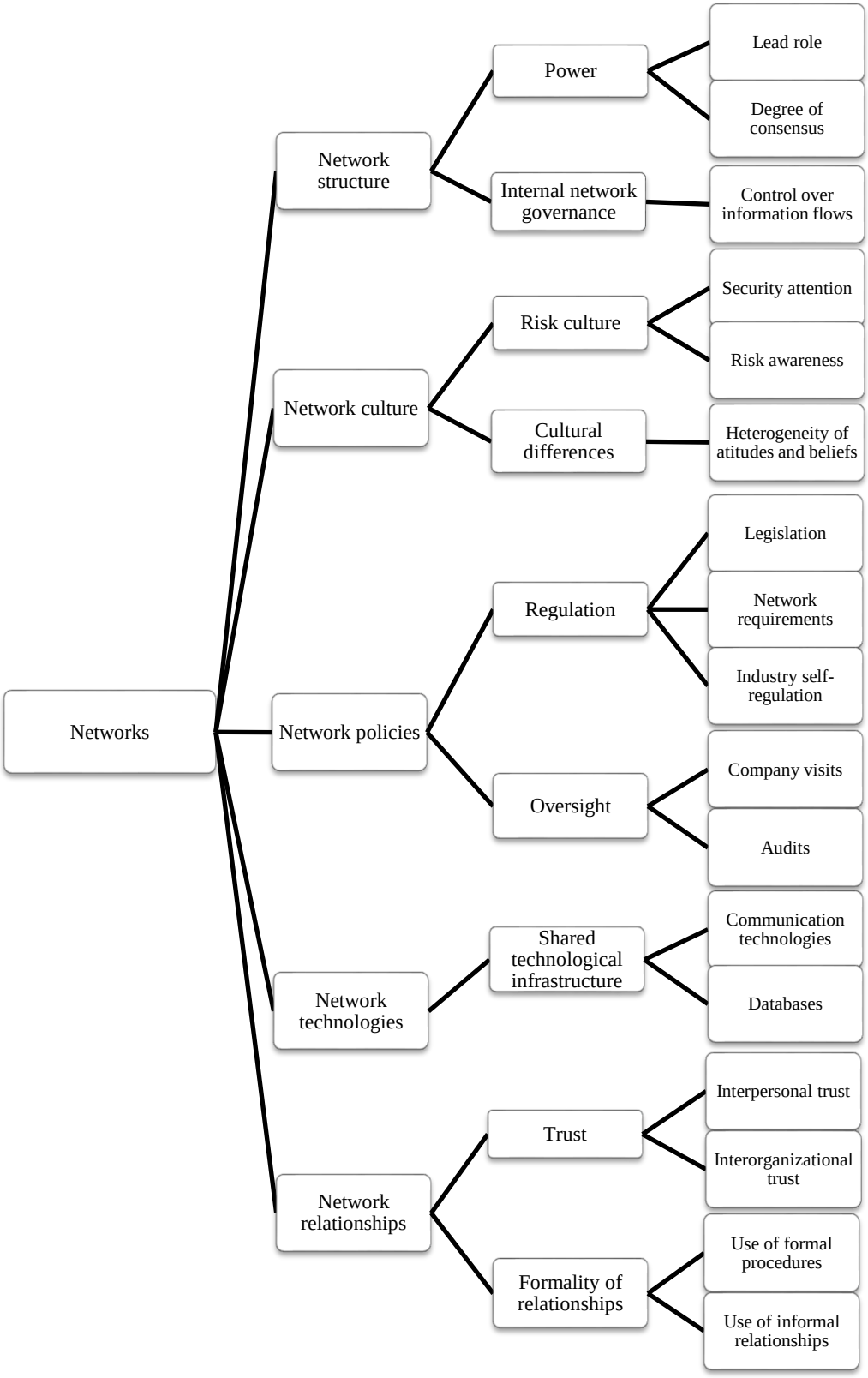

Figure 2: Operationalization chart.

3.4 Reliability and validity

For this section, it is important to notice that reliability and validity in qualitative research are different from reliability and validity in quantitative research (Bryman, 2012: pp. 389-390; Neuman, 2014: p. 218). As this study is a qualitative study, it will adhere to the notions of reliability and validity for qualitative research.

3.4.1 Reliability

Reliability in qualitative research is concerned with making stable and consistent observations (Neuman, 2014: p. 218). By applying the same analytical framework to the situation before and after the DigiNotar crisis, the data analysis builds on the same observational thoughts. Furthermore, a large part of the study is concerned with well-documented past events, which should benefit the reliability of the study.

The study also intends to gain knowledge about the current state of affairs, a part that might be more subject to the interpretations of the researcher. However, different interpretations can also lead to different, new insights on the elements studied. It is therefore accepted that a qualitative study is not as replicable and not as rigid in its methods as a quantitative study.

3.4.2 Validity

Validity in qualitative research is about offering a truthful, authentic account of the phenomenon or process studied (Neuman, 2014: p. 218). This study's validity is sought for in multiple ways. First, validity should benefit from the conceptualization of the study's main concepts, based on a balanced account of academic literature of respected scholars. Second, the DigiNotar crisis and the PKIoverheid system will be studied through a variety of sources, ranging from government records to independent inquiry reports, and from government officials to private stakeholders. This is expected to contribute to a balanced perspective.

External validity in the respect of generalizability is not the aim of this study, as the study seeks to provide insights on a specific crisis and its consequences. However, it is expected that the study might generate results that can be applied to public-private partnerships in the larger domain of cyber security, in the Netherlands or even beyond. The study's reflection will address this.

4. Analysis

This part will answer the three sub questions, starting with an analysis of the DigiNotar crisis and the context in which it took place. The chapter will then continue by answering the other two sub questions, using the analytical framework as set in out in chapter 2.3.1. Finally, the characteristics of public-private partnerships will be compared and conclusions will be drawn.

4.1 The DigiNotar crisis and its context

This segment will discuss the events and the context of the DigiNotar crisis and will answer the first sub question: *What was the DigiNotar crisis?*

To fully understand the crisis, this chapter will first discuss DigiNotar as a company and its role as a certificate authority. Subsequently, this section will expand on the events of the DigiNotar crisis and it will look into the aftermath of the crisis. The content of this chapter will contribute to a better understanding of the significance of the DigiNotar crisis to the public-private partnerships that constitute the PKIoverheid system.

4.1.1 The company DigiNotar

Encouraged by the Royal Dutch Association of Civil-law Notaries (KNB), DigiNotar was founded in 1997 as a private company. With digital technology spreading rapidly, DigiNotar was to play a key role in supporting civil-law notaries that wanted to use new, electronic means to provide their services. Among the first services of DigiNotar were the distribution of digital certificates, certified archiving, and the secure exchange of confidential documents (OVV, 2012: p. 36).

After a European directive on electronic signatures was issued in 1999, the provisions for the distribution for qualified digital certificates became more stringent and, since 2003, companies that wanted to engage in the distribution of such certificates had to sign up with the Dutch Telecommunications Authority (OPTA) (Van der Meulen, 2013: p. 51). DigiNotar registered at OPTA and slowly started to expand its services to other government agencies and services like the Dutch Tax and Customs Authority (Belastingdienst) and login credential service DigiD (Van der Kolk, 2011).

In 2004, when electronic filing of taxes became obligatory in the Netherlands, DigiNotar flourished and became a certificate authority for PKIoverheid certificates (De Jongh, 2007). PKIoverheid certificates established the trustworthiness of government

websites and secure communication between government agencies, between government and citizens, and between government and private organizations. DigiNotar became one of only six certificate authorities eligible to issue PKIoverheid certificates, as it was deemed to meet all the required security provisions for this task (Van der Meulen, 2013: p. 51; Rijksauditdienst, 2012: p. 9).

In January 2011, American information security giant VASCO Data Security International acquired DigiNotar for a price of 13 million US dollars. VASCO saw DigiNotar as a reliable company, which would become important to make the next step in offering digital certificate services (Martin, 2011). Under ownership of VASCO, DigiNotar continued fulfilling its tasks of certificate authority until the DigiNotar crisis led to the demise of the company. Before elaborating on the events of the crisis, the next section will line out the importance of digital certificates, in particular that of PKIoverheid, and the security implications that go with it.

4.1.2 Digital certificates

Since its inception, DigiNotar gradually expanded its services and provided digital certificates for a growing number of clients, ranging from the Dutch Ministry of Justice to mortgagor Hypotrust, and from Delft University of Technology to Dutch lawyers' association The Netherlands Bar (NOvA) (Fox-IT, 2012: pp. 84-90). This section will explain why these organizations needed digital certificates, and for what purpose.

Many websites give access to confidential information, financial services, or are designed to exchange or buy products and services. Malevolent actors could fabricate such a website or redirect an oblivious visitor to a different website, in order to obtain login credentials and to, for example, get access to bank account or credit card information. Browsers and operating systems are designed to check the trustworthiness of such websites by scanning for a digital certificate, issued by a reliable certificate authority. Browser and operating systems will warn its user when a website's digital certificate does not come from a reliable certificate authority (Wolff, 2016).

Digital certificates not only guarantee the reliability of websites. Digital certificates can also guarantee the authenticity, integrity, or confidentiality of e-mails, messages, files or programming code by providing a digital signature or by using encryption. For example, a digital signature can be verified by a digital certificate's publicly known key, which only recognizes the signature when the files are not altered or tampered with. Internet communication that is encrypted with a similar public key can be decrypted with a private

key that is only known to the recipient. This makes that digital certificates are important tools in securing confidentiality and trust in many forms of internet traffic (Van der Meulen, 2013: p. 47).

Because browser or operating system vendors do not have the capacity to check the trustworthiness of all companies and individuals that request a certificate, the issuance of certificates is done by trusted third parties, the certificate authorities. The core business of a certificate authority is to verify the entity or person that requests a digital certificate. The digital certificate then indicates the trustworthiness of the recipient of the certificate. The better the safeguards and the tighter the procedures of a certificate authority, the more reliable its certificates are considered (OVV, 2012: p. 50; Van der Meulen, 2013: p. 47).

4.1.3 PKIoverheid

By 2011, DigiNotar had built a solid reputation as certificate authority, issuing different types of certificates for a range of government and non-government websites or services (Wolff, 2016). Among these certificates were the PKIoverheid certificates. PKI stands for Public Key Infrastructure, a multi-component system that provides a mechanism for the issuance, storage, and distribution of digital certificates, public keys, and private keys (Maurer, 1996: p. 325).

The public key infrastructure landscape of the Netherlands then consisted of multiple certificate hierarchies, comprising so-called root certificates, intermediary certificates, qualified certificates, trusted third party certificates, and miscellaneous other certificates (Logius, n.d.). For example, to issue trusted third party certificates, a company needed a trusted third party (TTP.nl) declaration. To obtain a TTP.nl declaration, an accredited auditor had to do a management audit to check if management systems complied with a set of ETSI norms, developed by the European Telecommunications Standards Institute (Van der Meulen, 2013: pp. 51-52).

However, when a company wanted to issue the higher-in-rank qualified certificates, it needed the TTP.nl declaration, but it also needed a registration at Dutch telecom authority OPTA, that in 2011 fell under the responsibility of the Dutch Ministry of Economic Affairs, Agriculture, and Innovation (Logica Business Consulting, 2012: p. 22). OPTA then demanded the certificate authority to comply with a set of norms similar to those necessary for the TTP.nl declaration, and was made responsible for oversight on the certificate authorities that issued the qualified certificates (Van der Meulen, 2013: p. 52).

Then for the PKIoverheid certificates, again the TTP.nl declaration was necessary, but additional requirements and provisions were laid out in the Program of Requirements (Programma van Eisen), that was composed by Logius. Logius fell under the Ministry of Interior and Kingdom Relations (Logica Business Consulting, 2012: p. 25). Because of these extra requirements and the stringent oversight arrangements with Logius, the PKIoverheid certificates are high-ranked, Dutch government accredited certificates. For this reason, the PKIoverheid certificates yielded a very high level of trust, making the PKIoverheid certificates also an attractive target for the evil-minded (Wolff, 2016).

To counter attacks from outside, DigiNotar armed itself through a range of security measures. Approving certificate requests could only be done according to a four-eye principle; activating a private key for the approval of a certificate could only be done with physical smartcards that required a PIN code; and an employee's physical access to secured rooms was only possible when a second employee granted his access. Furthermore, biometric hand recognition systems and sluicegates managed the access to the rooms that stored the main servers and network devices of DigiNotar (Fox-IT, 2012: p. 19).

Despite all these security measures, the hacker did manage to breach DigiNotar's systems and to fabricate and issue rogue certificates, ultimately leading to the DigiNotar crisis. The next paragraphs will discuss the hack and the subsequent crisis in detail.

4.1.4 The DigiNotar hack

The investigation by Fox-IT shows that the first traces of hacker activity in the servers of DigiNotar relate back to June 17, 2011. On this date, the intruder gained entry to the external Demilitarized Zone - better known as DMZ - that separated the external and internal segments of the DigiNotar network. In the following days, the hacker succeeded in accessing the internal segments of the network and on July 10, the first rogue digital certificate was issued (Fox-IT, 2012: pp. 4-5).

On July 19, an internal check by DigiNotar exposed that 128 rogue certificates were issued. Another check on July 20 uncovered another 129 false certificates. This check used to run daily, but had not worked for some days for an undisclosed reason. As soon as the issuance of these false certificates came to light, DigiNotar revoked the false certificates and hired an external security company to investigate the breach and to rid the network of any intruder (OVV, 2012: p. 43).

Although DigiNotar had an obligation to report breaches to Logius, Dutch telecom watchdog OPTA, and the auditor that was concerned with granting the trusted third party

agreement, DigiNotar decided not to report the breach to these organizations. DigiNotar was convinced that the breach of its servers and the compromise of certificates were contained sufficiently, and that the events did not concern the PKIoverheid, qualified, or trusted third party certificates that were affiliated with Logius, OPTA or the trusted third party agreement (OVV, 2012: p. 44).

Until August 27, the situation seemed under control. False certificates had been revoked and the security breach was deemed fixed. But on that day, an Iranian Gmail-user under the alias Alibo posted a new thread in the Google Help Forum, in which he reported that Google browser Chrome had issued a certificate warning when he tried to access his Gmail account. He surmised that the Iranian government was snooping on its citizens. However, the certificate authority that had issued the certificate was the Dutch company DigiNotar (Alibo, 2011).

The German government's computer emergency response team (CERT.Bund) followed up on the forum post and reported it to its Dutch counterpart GOVCERT.nl, which notified DigiNotar, Logius, and the browser vendors (Van der Meulen, 2013: p. 48). DigiNotar immediately revoked the false certificate and announced a new investigation. DigiNotar informed Logius that there was no proof of any PKIoverheid certificates being compromised (OVV, 2012: p. 44).

On August 29, DigiNotar hired Dutch information security company Fox-IT to investigate how the false Google certificate could have been fabricated. Due to the urgency of the matter and the complexity of the PKIoverheid landscape, Fox-IT first produced a short report with preliminary findings. Fox-IT had found a total of 531 rogue certificates and reported that the security of all certificate authority servers had been compromised, but that it did not find evidence of misuse of the PKIoverheid certificates or the OPTA supervised qualified certificates (Fox-IT, 2011: pp. 7, 9).

Only one certificate authority server, for payment solutions in retail business, was not compromised, because the smartcard to generate a private key had been stored in a vault (Fox-IT, 2012: p. 57). However, because all other certificate authority servers and their log files had been accessible to the intruder, Fox-IT concluded that it was no longer possible to rely on the authenticity of DigiNotar's certificates and that, according to general PKI security standards, all DigiNotar certificates had to be revoked (Fox-IT, 2012: p. 46).

Fox-IT also found that the rogue Google certificate was created on July 10 and that until August 29 an estimated 300,000 Google users had encountered that certificate. Notable detail was that almost all requests for the rogue certificate originated in the Islamic Republic

of Iran. Fox-IT could not say with certainty, but the Gmail accounts of these Iranian users might have been compromised, meaning that not only their e-mails might have been intercepted, but that their login credentials could have been intercepted as well. This could provide the hacker access to mailbox and, for instance, an opportunity to access other services like Facebook, Twitter, or Google Docs, implicating the heaviest of consequences for Iranian citizens and, more particularly, Iranian dissidents (Fox-IT, 2011: p. 8).

Further investigation also exposed that the hacker had issued false certificates for the website hosting and e-mail service provider domains of *.wordpress.com, login.live.com, and login.yahoo.com, but also for the politically more sensitive domains of www.mossad.gov.il, www.cia.com, and www.sis.gov.uk. Additionally, the intruder had left a message, bragging about his hacking skills and leaving the signature of Janam Fadaye Rahbar (Fox-IT, 2011: p. 13). This signature also popped up during the investigation of a similar breach at the American certificate authority Comodo, earlier in 2011, and is a popular battle cry among the Iranian Revolutionary Guard, meaning "I will sacrifice myself for the Great Leader" (NOS, 2011).

Despite these signals, it was too early to attribute the attack to an individual or to label it state-organized or state-sponsored. And more important, the first priority was damage control. Now the PKIoverheid certificate authority server of DigiNotar had been compromised, the Dutch Ministry of Interior and Kingdom Relations had lost trust in DigiNotar and took the extraordinary measure to take over operational management of the company to restrict further damage to the integrity of the PKIoverheid system and to internet traffic in general (Ministerie van Binnenlandse Zaken & Koninkrijksrelaties & Ministerie van Veiligheid en Justitie [MinBZK & MinVenJ], 2011a: p. 1). In turn, Logius also had lost trust in DigiNotar and immediately wanted to revoke the PKIoverheid license of DigiNotar and all the certificates that were issued under it (OVV, 2012: p. 48).

Yet, immediately revoking all of DigiNotar's PKIoverheid certificates would be a disaster. DigiNotar-issued certificates were integrated in a range of government and non-government services, in particular in Dutch tax filing applications. Immediately stripping DigiNotar of its PKIoverheid license and revoking all of DigiNotar's certificates was expected to seriously harm the continuity of various e-government services and would, for example, halt the flow of tax money to the government (OVV, 2012: pp. 47-48).

To mitigate such continuity issues, the untrusted certificates had to be replaced by new certificates of different certificate authorities first. In the meanwhile, the public was advised not to use e-government services until DigiNotar's certificates were replaced. The

risks that accompanied this course of action were accepted as affordable, but the trustworthiness of the Dutch government's digital services suffered a heavy blow, worldwide (Zetter, 2011).

As soon as the unreliable DigiNotar certificates were replaced by new certificates of different certificate authorities, the Dutch government openly withdrew its trust in DigiNotar and revoked its PKIoverheid license. Browser developers like Mozilla, Microsoft, and Google were a step ahead and had already blacklisted all of DigiNotar's certificates (Zetter, 2011).

The extraordinary erosion of trust hurt DigiNotar so badly that on September 20, 2011, the Haarlem court declared DigiNotar's bankruptcy (Boon, 2011). Whilst DigiNotar ceased to exist, the Dutch government started new investigations into the crisis and prepared measures to prevent such an incident from ever happening again.

4.1.5 The aftermath of the DigiNotar hack

Whilst some malfunctions were expected due to an upcoming Microsoft-patch, just a few municipalities experienced some minor disturbances. Still, some other organizations were not so lucky and had to change their daily operations, like the Dutch bar association NOvA, that had to switch from a digital to a physical exchange of documents with Dutch courts. A new system for the onboard computers of Dutch taxis was delayed as well, because it was built with DigiNotar's digital certificates (MinBZK & MinVenJ, 2011b: p. 2). In that respect, damage to society seemed to be marginal, but the Dutch government knew there was work to be done.

Whilst the crisis was being resolved, the responsible Dutch ministries announced measures to prevent such a crisis from happening again. The Secretary of State for Security and Justice was to submit new legislation that would introduce a reporting requirement for security breaches similar to that of DigiNotar, the recently formed Cyber Security Council would be consulted for advice on maintaining the security and integrity of data communication, and recent developments would be taken into account during the development of a new national cyber security strategy (MinBZK & MinVenJ, 2011a: pp. 6-7).

Within another two weeks, the same Dutch ministries suggested a three-way approach to reduce the vulnerability of digital data communication. The three axis were (1) reinforcing the defense against cyber attacks; (2) increasing resilience in the case an attack succeeds; and (3) structural changes on a global level. In particular for the reinforcement of cyber defense,

the Dutch government had to strive for better cooperation between public and private parties and announced to expand relevant knowledge, to foster security awareness, and to create new arrangements for oversight and the of reporting incidents (MinBZK & MinVenJ, 2011b: pp. 3-4).

Yet, these announcements left one of the most important questions about the DigiNotar crisis unanswered: how could an attack on a highly secured and trusted government partner like DigiNotar happen and go unnoticed to the government for such a long time? To address this question, a number of technical and procedural investigations was ordered. The technical investigation of the DigiNotar hack was continued by Fox-IT, an overall evaluation of the PKIoverheid system was performed by Logica Business Consulting, and procedural investigations were executed by government audit service Rijksauditdienst (RAD) and the Dutch Safety Board (OVV) (MinBZK, 2012a: pp. 1-2).

4.1.6 The Fox-IT investigation

The technical investigation by Fox-IT shed more light on the techniques the intruder used to bypass DigiNotar's security systems, but also showed how DigiNotar failed to fully maintain the security of its network. The investigation exposed that the hacker had gained entry by using known security vulnerabilities of outdated software that was running on the external servers of DigiNotar, and used this entry as a stepping-stone to the internal part of the network on which the certificate authority servers ran. When the software had been up to date, the hacker could not have used these vulnerabilities (Fox-IT, 2012: pp. 23, 56).

Additionally, the automated routine tests that verified recently issued certificates had failed from July 10, 2011 until July 19, 2011. Also, logs that registered issued certificates were not stored on a separate server. This meant that the intruder also had access to the logs and had the opportunity to tamper with them or to cover its tracks (Fox-IT, 2012: p. 37).

Earlier findings of Fox-IT had already indicated that security had been weak due to the usage of weak passwords, the absence of proper anti-virus software, missing software updates, and access to all servers once inside the system. Most security flaws could have been prevented by adequate updates and improvements, implicating that a great deal of culpability rested on DigiNotar (Fox-IT, 2011: p. 9).

4.1.7 The Logica Business Consulting study

The Logica Business Consulting (Logica) study focused on the role of DigiNotar in the PKIoverheid system. Logica - later acquired by CGI - also concluded that the management of

DigiNotar had failed to implement security standards that could be expected from an organization engaged in such a vital part of information security (Logica Business Consulting, 2012: p. 5).

Furthermore, Logica concluded that oversight arrangements were insufficient as too much trust was placed on the TTP.nl declaration, that risk analyses were still in a premature stage, and that security norms and requirements of the PKIoverheid system were too complex and sometimes too unspecific to check various aspects of information security (Logica Business Consulting, 2012: p. 6).

The Logica study did not make specific recommendations to improve the partnerships within the PKIoverheid system, but it discussed the importance of market forces in the provision of digital certificates in general, and how oversight and trust play a key role when outsourcing digital certificate services (Logica Business Consulting, 2012: pp. 79-81).

Logica also discussed alternatives for the PKIoverheid system, but acknowledged that these alternatives were no proven successes yet. The reliability of public key infrastructure, already an intricate system, remained largely dependent on complex concepts like trust and the human factor (Logica Business Consulting, 2012: pp. 80-82).

4.1.8 The Rijksauditdienst report

The Rijksauditdienst (RAD) is the audit service of the Dutch government, and is part of the Ministry of Finance. The scope of RAD's audit was on the behavior and the performance of the Dutch government with regard to the DigiNotar crisis. Similar to Logica, RAD found that oversight was largely built on trust and questioned if such an oversight arrangement should hold after the events of the DigiNotar crisis (Rijksauditdienst, 2012: p. 8).

RAD also pointed out the lack of a systematic risk analysis, the absence of a crisis protocol, and an insufficient overview of the certificates issued by each certificate authority (Rijksauditdienst, 2012: pp. 8-9). On the other hand, RAD lauded the Dutch government for taking over operational management of DigiNotar and for adequately bringing together key players in an effort to mitigate the impact of the DigiNotar crisis (Rijksauditdienst, 2012: pp. 12-13).

RAD concluded its report by stressing that whilst the government tended to outsource cyber security tasks to private actors, it should take in more of these tasks itself and it should expand specific knowledge within the government (Rijksauditdienst, 2012: p. 14).

4.1.9 The Dutch Safety Board investigation

The Dutch Safety Board (OVV) is a non-profit and independent inquiry board that investigates situations in which the security of citizens depends on the government, companies or other organizations. OVV was approached by the Dutch government to conduct an investigation of the DigiNotar crisis, a customary procedure after a large security incident (OVV, 2012: p. 2).

In its report, OVV condemned DigiNotar for not acting upon the earliest signals of the breach and for the flaws in their security, as exposed by Fox-IT. However, OVV also pointed out that Logius and OPTA did not regularly audit DigiNotar themselves. Both organizations trusted on the TTP.nl audits that were ordered by DigiNotar and were performed by an accredited private auditor. These audits never gave reason to doubt DigiNotar's security, neither did the due diligence check by VASCO (OVV, 2012: pp. 38-40).

The audits gave the impression that DigiNotar was a reliable certificate authority, but OVV stated that the audits only checked whether the management systems were compliant to the required norms, were too unspecific, and were not adequate to assess the responsibilities DigiNotar had as PKIoverheid certificate authority (OVV, 2012: p. 42). OVV stated that the audits were irresponsible for digital certificate services, particularly those that have to adhere to PKIoverheid norms. OPTA and Logius should have shown more involvement in the operations of DigiNotar, and with the possible risks that came with these operations (OVV, 2012: p. 58).

OVV established that the DigiNotar crisis was caused by problems on the public and on the private side of the partnership, and that there seemed to be a tendency that government executives left important matters of cyber security to ICT-professionals by a lack of own understanding. Crucial cyber security decisions therefore tended to be made by ICT-professionals rather than by the responsible executives, creating discrepancies in the awareness of risks (OVV, 2012: pp. 84-85).

OVV concluded its report by stating that the government is responsible for cyber security at government organizations, but also for cyber security of society as a whole. And now, as the risk that a private party causes digital damage has been proven real, the government should intensify its efforts to create awareness of such risks, to stimulate cyber security improvements inside and outside government, and to take greater responsibility in order to reduce the chances of a new cyber crisis (OVV, 2012: p. 86).

4.1.10 Government response to the investigations

The Minister on Interior and Kingdom Relations responded to the reports by Logica and RAD in a letter to the House of Representatives on March 14, 2012. In response to the Logica-report, the Minister announced to clarify the norms for audits, to better define the division of roles between auditors and oversight bodies, to enforce more active involvement of OPTA and Logius, to make threat assessments more regularly, and to actively consult with private actors that offer digital certificate services (MinBZK, 2012b: pp. 3-4).

The Minister responded to RAD's findings by stating that the DigiNotar breach changed the way of thinking about cyber security and had brought together public, private, and international organizations in the field of cyber security. The Minister also acknowledged that the continuity of online services comes in jeopardy when digital certificates are revoked, and that measures involving this continuity deserve more attention in the near future (MinBZK, 2012b: pp. 5-6). The Minister concluded his letter by signaling that changes in the role of government are necessary to keep up with technological progress (MinBZK, 2012b: p. 7).

There was no formal government response to the Fox-IT report, which was only provided as an attachment to a short statement in a letter to the House of Representatives (MinBZK, 2012c: p. 3). However, Fox-IT's findings were extensively used in the OVV report, to which the Minister of Interior and Royal Affairs did respond elaborately.

In response to the OVV's findings, the Minister acknowledged the importance of information security and of adequate emergency protocols, and dubbed the DigiNotar crisis a wake-up call. The letter was addressed to the president of the OVV, but a copy was sent to the House of Representatives. Together with the *Lektober*-experiences, during which website *Webwereld* published privacy issues in government websites or services, the DigiNotar crisis had triggered extra government commitment to enhance Dutch cyber security (MinBZK, 2012d: p. 1).

In that same letter, the Minister announced the commission of a task force to change the general mindset of managers and board members regarding cyber security. The task force was to work together with the recently installed NCSC to create a national and multi-sector response network to increase cyber resilience. For the same purpose, new legislation would be implemented that would require the reporting of security breaches at organizations in the government, in the financial sector, and in other organizations that shape important preconditions for everyday life (MinBZK, 2012d: pp. 2-4).

Concerning the field of digital certificate services, the Minister made clear that audit arrangements between Logius, OPTA, and the accredited auditors had already been changed, that the requirements for PKIoverheid had been rewritten by Logius, and that Logius and OPTA from then on would regularly visit the certificate authorities to reinforce their oversight. Additionally, Logius was going to perform yearly penetration tests at the PKIoverheid certificate authorities and would underline the importance of security breach notifications. In other words, change was going to happen (MinBZK, 2012d: p. 4).

4.1.11 Consequences for VASCO

VASCO also had to cope with the aftermath of the DigiNotar crisis, now the millions they had spent to acquire the Dutch company had vanished. The endgame between VASCO and DigiNotar was played in the court of justice. VASCO, feeling like it had bought a pig in a poke, had sued the former owners of DigiNotar for failing to comply with necessary security standards. Closure came in 2014, when after months of litigation the court of Amsterdam ruled in favor of VASCO and ordered the former owners of DigiNotar to pay several millions of compensation (Van der Kolk, 2014).

4.1.12 Subsidiary conclusion

This chapter has provided an analysis of the DigiNotar crisis and has shed light on the context in which the crisis took place. DigiNotar was a private company, which had built itself a firm reputation as a certificate authority that issued, among others, highly trusted qualified certificates and PKIoverheid certificates. These certificates are used to secure internet traffic between government, citizens, and companies, and therefore are cornerstones of cyber security.

However, the hack of DigiNotar led to a compromise of these certificates and exposed failing security provisions in the DigiNotar networks. These failing security provisions were missed by auditors and oversight bodies, because they put too much trust in each other's assessments, but also because they audited more on management norms rather than on information security standards. The DigiNotar crisis was investigated by multiple organizations and was seen as a wake-up call for the Dutch government to improve its cyber security practices.

Shortly after the crisis, the Dutch government announced it would change oversight arrangements in the PKIoverheid system, it would introduce obligatory reporting of security breaches, and it would install task forces and additional networks to increase cyber resilience.

The aftermath of the DigiNotar crisis made clear that extra commitment by public and private parties was necessary to keep up with technological progress, and that this extra commitment was a prerequisite for securing an increasingly digitalized society.

4.2 Public-private partnerships before the DigiNotar crisis

This chapter will answer the second sub question: *What were the characteristics of public-private partnerships in the PKIoverheid system before the DigiNotar crisis, and how does this relate to the events of the DigiNotar crisis?* The thesis uses the analytical framework as developed in chapter 2.3.1 to study each level of analysis individually. Data stems from official policy documents, from reports of the DigiNotar crisis, and from interviews held with relevant stakeholders. Extracts from the interviews can be found in the appendix.

The next section will first generally address the Dutch cyber security to provide a basic context of the state of affairs of the Dutch cyber security landscape. Later, this chapter will zoom in on public-private partnerships in the PKIoverheid system. The results of this chapter will provide a reference point to study to what extent these public-private partnerships have changed in response to the DigiNotar crisis.

4.2.1 The Dutch cyber security sector

Just months before the DigiNotar crisis, the Dutch government published its first official national cyber security strategy, in which it set out the government's course of action to keep up with recent developments and to counter threats that exposed the dependence of society on information technology. Some of the threats that were identified by the Dutch cyber security strategy were the Stuxnet malware, the massive botnet Bredolab, and an increase in DDoS-attacks (NCTV, 2011: p. 1).

Regarding digital developments in the Netherlands, the Netherlands Scientific Council for Government Policy (WRR) established in early 2011 that the Dutch government was embracing all sorts of digital advancements, but that its policy on the use of information flows and information technology was often characterized by ad hoc and incoherent decision making, lack of ownership, and a lack of awareness of the consequences and risks of digitalization (WRR, 2011: pp. 14-15). The latter was also indicated by the OVV, which had stated that decision making often did not take place at strategic level by the managers – due to a lack of ICT knowledge - but was done at operational or tactical level by ICT experts (OVV, 2012: pp. 84-85).

To counter recent developments, the cyber security strategy specifically mentioned the necessity of cooperation between public and private parties, with a clear division of roles and responsibilities, and a key role for trust and reciprocity. According to the cyber security strategy, public and private should cooperate as equals and each party should benefit from joint initiatives (NCTV, 2011: pp. 3-4).

What also stood out in the first cyber security strategy was the foundation of the Cyber Security Council (CSR) and the National Cyber Security Center (NCSC). These two organizations had to play a key role in bringing public and private parties together and in coordinating joint cyber security initiatives, from strategic to operational level. The NCSC would incorporate the existing GOVCERT.NL and would harbor the then still to be formed Incident Response Board (NCTV, 2011: pp. 5, 8).

The 2011 cyber security strategy being the first Dutch cyber security strategy - and much of the plans to create cyber security mechanisms still being in the pipeline - indicate that the Dutch cyber security landscape was still young when the DigiNotar crisis unfolded. Whilst the use and importance of information technology rapidly became more important, risk awareness at strategic level was rather low and coordinating mechanisms differed per department or per partnership, if present at all. Dutch government had started efforts to guide the digitalization in the right way, but it was not quite there yet.

This development is probably demonstrated best by the results of the interviews that were conducted for this study. For instance, the senior coordinating advisor of the NCSC confirmed the findings of the OVV and stated that most expertise on cyber security back then rested with ICT experts, not yet with the executives that made decisions at strategic level. Only slowly - with the DigiNotar crisis creating much more awareness - cyber security started to reach the boardrooms (senior coordinating advisor NCSC, personal interview, May 1, 2018: transcript S1).

For some sectors (e.g. the financial sector), non-physical Information Sharing and Analysis Centers (ISAC's) had been set up to facilitate all-channel exchange of information on cyber security, whilst other sectors still had to develop plans for such a collaboration. The development of ISAC's also depended on the culture and the uniformity of the sector. In other words, public-private partnerships need to be customized to the specific needs and characteristics of the sector in which the parties operate (senior coordinating advisor NCSC, personal interview, May 1, 2018: transcript S2).

As public-private partnerships have to be tailored to these specific needs and characteristics, it is hard to study public-private partnerships in the cyber security sector in a general fashion. The partnerships in form of ISAC's can differ strongly from partnerships in which there is a product to be delivered, like in the more specific field of digital certificate services. Therefore, this study will look specifically into the public-private partnerships that constitute the PKIoverheid system.

4.2.2 Network structure

Before and during the DigiNotar crisis, the Dutch Ministry of Interior and Kingdom Relations was responsible for the PKIoverheid system and had appointed Logius as the autonomously operating policy authority (senior official MinBZK, personal interview, May 14, 2018: transcript S3). Logius therefore reported to the Ministry, but managed the PKIoverheid system tactically and composed the requirements (Programma van Eisen) for the public and private parties that issued the PKIoverheid certificates. Logius did not issue any PKIoverheid certificates itself (OVV, 2012: pp. 55-56).

Furthermore, Logius performed oversight on the providers of the PKIoverheid certificates. The private certificate providers issued the PKIoverheid certificates on the basis of a contract with Logius (Logica Business Consulting, 2012: p. 19). As Logius operated on behalf of the Dutch government in these public-private partnerships, Logius was the policy authority of the PKIoverheid system (coordinator eIDAS oversight AT, personal interview, May 22, 2018: transcript S4).

Within the PKIoverheid system, qualified certificates were issued as well. OPTA, the Dutch telecom authority that operated under the Dutch Ministry of Economic Affairs, Agriculture and Innovation, was responsible for oversight on the providers of qualified certificates. Also, any party that wished to participate in the PKIoverheid system had to register at that same OPTA. The Ministry of the Interior and Kingdom Relations and the Ministry of Economic Affairs, Agriculture and Innovation thus had overlapping oversight responsibilities towards the private parties in the PKIoverheid system (Logica Business Consulting, 2012: p. 73; Rijksauditdienst, 2012: p. 7). The section on network policies will further explain how this oversight was arranged.

At first, this structure with the government agencies as administrators or supervisors over the autonomous certificate providers seems rather hierarchical, but Logius, OPTA and the private actors that issued PKIoverheid certificates shared the objective to issue reliable digital certificates and to maintain the reliability of these certificates. All parties were well aware of this objective (policy authority Logius, personal interview, April 25, 2018: transcript S5).

Next to a high degree of goal consensus, the public-private partnerships involved regular exchange of information about the requirements for digital certificates and periodic meetings between the Ministry of Interior and Kingdom Relations, Logius, and the certificate authorities. Such meetings were held once per three months (senior official MinBZK, personal interview, May 14, 2018: transcript S6). These arrangements also correspond with

Whelan's (2011) statement that a network "involves repetitive exchanges between a set of autonomous but interdependent organizations in order to achieve individual and shared objectives" (pp. 276-277).

When establishing whether internal network governance is shared or brokered, or whether the network is hub or all-channel, the hierarchy of the PKIoverheid system and the role of Logius as policy authority point toward a brokered network. Although the Ministry of Interior and Kingdom Relations is responsible for PKIoverheid, Logius was the organization that dictated the requirements, set up meetings, decided on the course of action, and clarified new provisions in the program of requirements (policy authority Logius, personal interview, April 25, 2018: transcript S7; commercial director QuoVadis, personal interview, May 9, 2018: transcript S8).

When applying the analytical framework the network structure resembles a hub, as Logius is the lead organization that holds the most power and decides on the course of action. It does report to the Ministry of Interior and Kingdom Relations, but was granted substantial freedom to manage day-to-day operations. Goal consensus was present, but maintaining trust in the system was also the most important imperative for the most influential organization Logius. This corresponds largely with the lead organization-governed network that Provan and Kenis (2008) have introduced, where the leading organization holds asymmetrical power and decides on the network's undertakings towards the network's goals.

4.2.3 Network culture

When the reports of the inquiries by OVV, RAD, and Logica were published, there was widespread criticism on the organizational culture with regard to security attention and risk awareness. RAD blamed in particular Logius for the lack of an extensive risk analysis and an adequate crisis mitigation strategy (RAD, 2012: pp. 8-9). Logica also concluded the absence of overarching risk management and argued that improved and integral risk management could prevent similar incidents from becoming a crisis (Logica Business Consulting, 2012: p. 76).

Furthermore, OVV stressed the importance of risk awareness in running effective security management and criticized the insufficient efforts of the involved parties to study scenarios that could endanger the security or integrity of the certificates. If such scenarios were studied at all, these were only limited to the own organization. This fragmented perspective on risk - or risk management - was demonstrated by Logius' plan to withdraw the trust in DigiNotar after the breach and to invalidate its certificates as soon as possible. Such a

plan would seriously disrupt the continuity of other digital services that were essential to society or government operations (OVV, 2012: pp. 61-62).

To make it worse, government boardrooms had only little awareness of security risks, because ICT knowledge mainly rested with technical experts. This negatively influenced strategic decision making on cyber security matters. This lack of expertise at executive level also was one of the main conclusions of the OVV report. Freely translated, the title of the OVV inquiry report was "Why cyber security does not reach the boardroom sufficiently" (OVV, 2012: front page).

The lack of security attention and risk awareness is also displayed in the way DigiNotar managed the security of its computer systems and how it interpreted its obligation to report security breaches. The Fox-IT report exposed that security had been weak due to the use of simple passwords, the absence of adequate anti-virus software, and the fact that vital software updates were missing (Fox-IT, 2011: p. 9).

This continued after the hack, as DigiNotar first falsely assumed that the servers that issued qualified and PKIoverheid certificates were not compromised and that it had acted accordingly by revoking all rogue certificates that they had encountered. OVV judged that the importance of security in the field of digital certificate services was enough reason for DigiNotar to inform its partners. Not only for the sake of early detection of possible similar threats, but also because it would provide an opportunity for all parties involved to learn from the incident (OVV, 2012: pp. 43-44).

Also problematic was how OPTA and Logius trusted on the audits by the accredited auditor that granted the TTP.nl declaration. OVV established that OPTA and Logius mainly used the TTP.nl audit to grant the PKIoverheid license. However, the TTP.nl audit mainly checked if management systems conformed to the ETSI norms, and did not specifically audit the certificate authorities for additional requirements related to their daily business operations (OVV, 2012: pp. 60-61).

Logius' current policy authority, then responsible for operational management at Logius, confirms this. When Logius received the audit report by the accredited auditor and found no irregularities, it would renew the PKIoverheid license with a year without doing much additional checks itself. After a year, a new TTP.nl audit would determine if the certificate authority still complied with the applicable ETSI and PKIoverheid requirements and Logius would trust the accredited auditor's judgment on this (policy authority Logius, personal interview, April 25, 2018: transcript C1). OPTA followed a similar course of action (coordinator AT, personal interview, May 22, 2018: transcript C2)

To establish if back then such an organizational cultural was exemplary for the whole PKIoverheid system, the other private parties in the PKIoverheid system were interviewed about this as well. One executive stated that Logius should rely only on facts, whereby healthy skepticism is logical. In the case of DigiNotar, there was too much trust and that was wrong (founder and CTO Digidentity, personal interview, May 1, 2018: transcript C3).

Another executive added that his company always maintained high risk awareness, because digital certificate services were their core business. A security incident would harm the reputation of his company so badly that it would probably threaten its existence (commercial director QuoVadis, personal interview, May 9, 2018: transcript C4).

A consultant at another trusted service provider explained that security standards at his organization already were high, because his organization also issued certificates accredited by American internet giant VeriSign. The strict rules VeriSign imposed on their affiliates had led to high security attention and risk awareness, and these strict rules were also applied to the issuance of PKIoverheid certificates (consultant KPN, personal interview, May 24, 2018: transcript C5).

In particular the first two statements were proven by the DigiNotar crisis, as the crisis first proved that the trust in DigiNotar was unjustified and, second, the crisis led to DigiNotar's bankruptcy within only a month after the crisis had made headlines.

The previous sections have shown that goal consensus was high and the involved parties knew the importance to maintain the trust in the PKIoverheid system. Still, some cultural differences existed, in particular when it came to security attention and risk awareness. It can be argued that these cultural differences did not directly influence the network's performance, but it was the sum of low risk awareness, ineffective oversight, and not fully complying with adequate security standards at or by mainly DigiNotar, OPTA, and Logius that contributed to the DigiNotar hack becoming a crisis. In section 4.3.3 it will be interesting to see how culture regarding security and risk awareness has developed after the crisis was resolved.

4.2.4 Network policies

Whelan (2011) explained that the focus of network policies is on the formal policies and procedures that prescribe the courses of action for the network participants (p. 280). In other words, the network policies are to guarantee a certain degree of control over the network, necessary to manage the risk that the public and the private share. Whelan (2011) also proposed that a network with critical objectives and high failure costs needs a clear policy

framework (p. 281). When looking at the field of digital certificate services and its importance for secure internet traffic, this thesis posits that this field qualifies for such a type of network. This section will now take a closer look at the policy framework in which the public-private partnerships in the PKIoverheid system operated.

In a broad sense, private parties that issued qualified and PKIoverheid certificates had to comply with the norm sets of Logius, OPTA and the accredited auditor that decided on the TTP.nl declaration. To check whether the certificate authorities indeed were compliant, these three parties had duties of oversight, executed mainly in the form of audits. Logius had to check if the parties that issued PKIoverheid certificates complied with their program of requirements (Programma van Eisen), OPTA was responsible for checking if providers of qualified certificates complied with Dutch telecom law (the Telecommunicatiewet, that had incorporated regulations from the 1999 European Commission directive for electronic signatures), and the accredited auditor checked if the certificate authorities complied with TTP.nl and ETSI norms (Rijksauditdienst, 2012: p. 7-8; Van der Meulen, 2013: pp. 50-51).

However, the TTP.nl declaration, which Logius and OPTA relied on heavily, only implicated a justified confidence by the accredited auditor that the certificate authority abided by active legislation. This was based on auditing whether management systems complied with the ETSI norm set, and not necessarily whether the certificate authority actually complied with all other legislation. Furthermore, the TTP.nl scheme did not prescribe in detail how the auditor had come to its decision or on which judgments the decision was made. Instead, the audit report only showed deviations from the norms (OVV, 2012: p. 58, 60).

The interview at Logius confirms the issues with norms and oversight, as it learned that had the government actually visited DigiNotar periodically, it would have got a much better sense of what was going on in the company. Possibly - or probably - the government had been able to identify more quickly any problems at DigiNotar. The obvious lesson learned was not to exclusively trust on the auditor's judgment whether a company was compliant with all rules and legislation, but to actively audit on site (policy authority Logius, personal interview, April 25, 2018: transcript P1).

A broad range of network policies - including duties of oversight and auditing - to manage and mitigate risk and to maintain network control thus did exist, but were not enforced sufficiently. This thesis supports what OVV at the time concluded: the risks that digitalization brings were not assessed accordingly and the government, the organization ultimately responsible for national cyber security, had not taken enough initiative to enforce

the policies that were designed to achieve a satisfactory level of cyber security, and to protect the public interest, that was becoming increasingly dependent on digital means (OVV, 2012: p. 85).

4.2.5 Network technologies

Whelan's (2011) framework describes network technologies as the technological means for effective information exchange between the network members. Such technologies can improve the shared situational awareness of the network, which can facilitate reaching the network goals and can benefit the network effectiveness (Boersma, Wagenaar & Wolbers, 2012: p. 3).

When studying the reports and interviewing the respondents, it quickly became clear that, apart from regular e-mail traffic, there were no shared technological means that facilitate information exchange and that there were no shared databases that, for example, list all PKIoverheid certificates issued. This is illustrated best by some of the responses on the question whether shared technologies are used:

> Founder and CTO Digidentity: *"No, none at all."* (personal interview, May 1, 2018: transcript T1)

> Commercial director QuoVadis: *"No, everyone has its own implementation of its certificate services."* (personal interview, May 9, 2018: transcript T2)

> Policy authority Logius: *"No, we have thought about tooling, but basically everything goes by e-mail."* (personal interview, April 25, 2018: transcript T3)

> Coordinator AT: *"We communicate by e-mail and by phone. As for the rest, there is no shared infrastructure."* (personal interview, May 22, 2018: transcript T4)

Interestingly, RAD listed among the key issues of the DigiNotar crisis the absence of a database in which all PKIoverheid certificates are registered. Such a database would have eased the process of tracing which services or websites used the PKIoverheid certificates and would have contributed to a quicker impact assessment when revoking the DigiNotar certificates (Rijksauditdienst, 2012: p. 9). OVV also saw the lack of overview of

compromised digital certificates as a complicating factor in maintaining the continuity of other digital services when the DigiNotar certificates had to be substituted (OVV, 2012: pp. 47-48).

Study of shared technologies before and during the DigiNotar crisis showed that the network members mainly use e-mail to communicate or to exchange information. However, a (shared) database that would have provided an overview of all issued certificates per certificate authority was deemed useful by OVV and RAD for quickly substituting compromised certificates and thus for quickly resolving the DigiNotar crisis. Still, the network effectiveness does not seem to suffer from the absence of shared technological means, as there is no necessity for shared technologies in day-to-day operations.

4.2.6 Network relationships

Whelan (2011) argued that network relationships touch upon the formal and informal relationships between the individuals and the organizations that are part of the network (p. 282). Furthermore, the more interdependence between the actors in the network, the more important trust becomes. When the level of trust is high, it is more likely that problems in the other fields - structure, culture, policies, and technologies - are overcome. Informal relationships can play a strong role in solving such problems (Whelan, 2011: p. 282).

The importance of relationships is also underlined by the interviewees. For example, the senior NCSC official that coordinates cyber security partnerships stated that good relationships, formal or informal, are essential for a quick exchange of ideas or the solution of imminent problems (senior coordinating advisor NCSC, personal interview, May 1, 2018: transcript R1).

The commercial director of QuoVadis agreed on this and said that it sometimes is easier to clarify ambiguities by making a phone call rather than by following a formal procedure. As PKIoverheid is a small world, everybody in the system exactly knows who is who (commercial director QuoVadis, personal interview, May 9, 2018: transcript R2).

The senior official of the Ministry of Interior and Kingdom Relations confirmed the importance of trust and said that, in particular in the field of security, trust is a key element and is essential in getting information. The senior official added that managing relations, knowing each other, and talking to each other is the way to get to know things (senior official MinBZK, personal interview, May 14, 2018: transcript R3).

The policy authority at Logius answered that he knew all important stakeholders personally, but that relationships are also within the context of the contracts between Logius and the

certificate authorities. He added that the number one objective remains to maintain trust in the PKIoverheid system and that he will take the necessary measures to ensure that objective. Nevertheless, meetings about the program of requirements always proceed in good harmony and the Dutch have always been good in reaching an acceptable degree of consensus (policy authority Logius, personal interview, April 25, 2018: transcript R4).

The consultant at KPN expressed that his relationships with the public and private participants in PKIoverheid are good, but that contact basically is restricted to the meetings with Logius about the program of requirements. Apart from that, there is no real interaction (consultant KPN, personal interview, May 23, 2018: transcript R5).

These extracts from the interviews indicate that the interpersonal relationships in the network, whether they are perceived formal or informal, have been good and can sometimes indeed contribute to solve problems or to clarify ambiguities in a quick fashion. However, sometimes interaction is only restricted to official meetings or is strictly in the context of the contracts. In any way, trust is considered as crucial in maintaining interpersonal relationships. The trust between organizations on each other's audits proved to be something different, as already has been shortly discussed in chapter 4.2.3.

Logius and OPTA placed too much trust in the accredited auditor by more or less directly accepting the audit report as good enough to renew the license of qualified and PKIoverheid certificates. The auditor was not directly to blame for this, as the auditor conformed to the TTP.nl scheme and the ETSI norms. However, because the audit reports were only building on these specific norms to establish the trustworthiness of only one component of the certificate authority, namely the management systems, Logius and OPTA were reproachable for placing too much trust on these audit reports (OVV, p. 42).

The interorganizational trust that Logius and OPTA then placed in DigiNotar was also largely misplaced, because the TTP.nl declaration was issued by an accredited auditor that was employed by DigiNotar itself. The government thus de facto trusted on the efforts of the certificate authorities to obtain a TTP.nl declaration. OVV labeled this as an irresponsible construction for a sector in which security and trust is crucial (OVV, 2012: p. 42).

Whilst trust and interpersonal relations between the network participants appeared to be good, and formal and informal relationships contributed to solve problems or to quickly communicate ideas and thoughts, the interorganizational trust that Logius and OPTA placed in the certificate authorities and in the accredited auditor clearly was inappropriate. Whilst interpersonal trust and relationships seem to have benefitted the network effectiveness, the

unjustified trust between organizations eventually undermined the effectiveness of the network, being one the factors that led to the DigiNotar crisis.

4.2.7 Subsidiary conclusion

Using the study's analytical framework, this chapter has evaluated the characteristics of public-private partnerships that operated in the PKIoverheid system before the events of the DigiNotar crisis unfolded.

The network structure of PKIoverheid can be defined as a hub, in which the Ministry of Interior and Kingdom Relations was responsible, but Logius operated as policy authority of the PKIoverheid system. OPTA had to provide for additional oversight on qualified PKIoverheid certificates, but was not part of the partnership. Logius was the lead organization of the network and decided on the course of action. Logius held power through bilateral contracts with each party. Such an arrangement resembles the lead organization-governed model as proposed by Provan and Kenis (2008).

The network culture was studied largely on the basis of security attention and risk awareness. This concerns not only the degree of security in the provision of reliable certificates, but also the overreliance on interorganizational trust, as Logius and OPTA almost blindly trusted the certificate authorities and its auditors. Security attention and risk awareness at these government agencies, but also at DigiNotar were too low for a sector in which security and adequate risk management were crucial. However, a lack of risk awareness was not exemplary for all PKIoverheid partnerships, as other private parties were well aware of security risks.

The network policies were defined by an extensive body of rules and legislation, on European and on national level. However, DigiNotar was not fully compliant with these norms and requirements. Additionally, ineffective oversight by Logius and OPTA failed to enforce that compliance, indirectly leading to security vulnerabilities.

Regarding network technologies, e-mail was the way to go for the exchange of information. There was no such thing as a shared database of, for example, all certificates issued under the PKIoverheid license, which later complicated the substitution of compromised DigiNotar certificates.

Network relationships differed strongly. Overall, interpersonal trust and interpersonal relationships, albeit formal or informal, were good and contributed to effective ways forward. Interorganizational trust on the other hand was problematic. Logius and OPTA placed large

amounts of trust in partnering organizations, which eventually proved to be destructive for DigiNotar and damaged the reputation and reliability of the PKIoverheid system.

Conclusively, network culture, network policies, and network relationships were the most vulnerable elements of the network, as the DigiNotar crisis can be seen as the result of inadequate risk awareness, failing oversight and compliance with norms, and overreliance on interorganizational trust. The next chapter will look into whether this has changed after the DigiNotar crisis.

4.3 Public-private partnerships after the DigiNotar crisis

This chapter will answer the third sub question: *What were the characteristics of public-private partnerships in the PKIoverheid system after the DigiNotar crisis, and how does this relate to the events of the DigiNotar crisis?* The thesis again uses the analytical framework as developed in chapter 2.3.1 to study each level of analysis individually. Data stems from official policy documents, news sources, and from interviews held with relevant stakeholders.

The first section will shortly address what the DigiNotar crisis has meant for public-private partnerships in the Dutch cyber security sector in general. The thesis will then continue by focusing on public-private partnerships in the specific domain of the PKIoverheid system.

4.3.1 The Dutch cyber security sector

After the DigiNotar crisis, the Dutch cyber security landscape changed significantly. On January 1, 2012, the Dutch national cyber security center (NCSC) started its activities to increase cyber resilience in the Netherlands. NCSC was and still is part of the National Coordinator for Security and Counterterrorism (NCTV), under the Ministry of Security and Justice (now the Ministry of Justice and Security). The Dutch computer emergency response team GOVCERT.NL became part of NCSC as well (NCSC, 2012).

Public and private parties united in or through the NCSC to bring together and to share knowledge and expertise on cyber security. ISAC's proliferated. First, NCSC would focus on vital sectors like telecom, energy, and water. Later, it was to gradually spread its wings to other sectors. The NCSC became the main party to monitor threats, to facilitate public-private collaboration in cyber security, and to respond to calamities (NCSC, 2012).

In 2013, NCTV also published a new national cyber security strategy. The Dutch Minister of Security and Justice Ivo Opstelten wrote in the introduction to the document that new developments in the cyber domain were coming fast and an adequate response was necessary. He also mentioned that the impact of cyber threats had become clearer after a number of incidents (NCTV, 2013: p. 3). He did not directly mention the DigiNotar crisis, but the crisis is mentioned in some of the document's footnotes (NCTV, 2013: p. 13-23).

The second national cyber security strategy thus does not directly mention a relationship between the changes in national policy on cyber security and the DigiNotar crisis. Changes in Dutch cyber security policy, and specifically on public-private partnerships, can better be seen in the light of an organic change towards more professional cyber security models. DigiNotar did change the mindset of politicians and those involved in

cyber security, but it did not directly lead to the creation of new directives or legislation. Self-regulation at that time was still preferred (senior coordinating advisor NCSC, personal interview, May 1, 2018: transcript P2).

The next paragraphs will explore what the DigiNotar crisis has meant for public-private partnerships in the field of PKIoverheid and how changes in the characteristics of these partnerships relate back to that crisis. The data from the interviews will play a key role in this and contains information about changes in the characteristics of public-private partnerships in the PKIoverheid system until June 1, 2018.

4.3.2 Network structure

After the DigiNotar crisis, Logius was heavily criticized for falling short of its role as the guardian of the PKIoverheid system. Still, Logius, as the digital government service, remains the policy authority of the PKIoverheid system and is entrusted with the administration and oversight of the PKIoverheid system. Logius still falls under the Ministry of Interior and Kingdom Relations, which is ultimately responsible for PKIoverheid (Logius, 2017: p. 9).

Logius remains to hold bilateral contractual relationships with the private parties that provide PKIoverheid certificates, and similar covenants with public parties that provide PKIoverheid certificates. These relations have hardly changed. Logius determines the course of action for the PKIoverheid system through their program of requirements and holds the power (policy authority Logius, personal interview, April 25, 2018: transcript S9).

Logius and the Ministry of Interior and Kingdom Relations still schedule meetings with the certificate authorities to discuss changes to their program of requirements or to gain support for certain decisions (Logius, 2017: p. 19; commercial director QuoVadis, personal interview, May 9, 2018: transcript S10). The Ministry of Interior of Kingdom Relations did intensify the frequency of those meetings after the DigiNotar crisis to once in two weeks instead of once per three months, but as the trust in the PKIoverheid system gradually restored, this frequency was eased again (senior official MinBZK, personal interview, May 14, 2018: transcript S6).

OPTA merged in 2012 into ACM, together with the Dutch consumer authority CA and Dutch competition authority NMa (ACM, 2011). Until the implementation of the eIDAS regulation, ACM was responsible for legal oversight on the providers of certificate services. However, when the European regulation on electronic identification, authentication, and trust services (eIDAS) was applied on July 1, 2016, ACM argued that the nature of oversight had changed to inspection, which they found did not fit their tasks that centered around market

regulation and consumer protection. Oversight duties then were transferred to the more technical Agentschap Telecom (AT) (coordinator AT, personal interview, May 22, 2018: transcript S11)

Since then, AT performs oversight on all Dutch providers of digital certificates and is mandated by the eIDAS regulation. AT does not directly oversee the certificates issued in PKIoverheid system. However, as the providers of PKIoverheid certificates also issue digital certificates that fall under eIDAS regulation, AT comes into play to check if these providers comply with that same eIDAS regulation (coordinator AT, personal interview, May 22, 2018: transcript S12). To reduce the burden of audit and to prevent duplication of effort, AT and Logius did agree to cooperate in performing oversight and signed a protocol to seal this agreement (Agentschap Telecom, 2017: p. 1).

By means of the eIDAS regulation, which will be discussed more extensively in chapter 4.3.4, the European Commission expanded its influence on digital certificate services. Provisions from the eIDAS regulation can now be found in Logius' program of requirements and have been implemented in Dutch telecom law. This can also be seen as part of a broader development, in which the European Commission has started initiatives to adopt cyber security standards and to monitor the implementation of these standards (senior official MinBZK, personal interview, May 14, 2018: transcript S13).

Another group that has gained power are the browser vendors, which have laid out requirements for the issuance of publicly trusted certificates by means of the Certificate Authority/Browser forum (or CAB Forum). Here, browser vendors like Google and Microsoft have united with certificate authorities worldwide and have set up the Baseline Requirements (CA/Browser Forum, n.d.).

The first edition of these requirements was published in 2011, shortly after the DigiNotar crisis, suggesting a direct link to the DigiNotar events. According to KPN's consultant, that indeed can be seen as a direct link (consultant KPN, personal interview, May 23, 2018: transcript S14). The policy authority at Logius confirmed this was a period in which the attention for securing digital certificate services gained momentum. Since then, these requirements are continuously updated and many have been implemented in Logius' program of requirements (policy authority Logius, personal interview, April 25, 2018: transcript S15).

So next to the requirements of Logius and AT, there is an increasing number of other conditions that the certificate authorities have to comply with. This is expressed in more stringent and more regular audits, which can be a burden to the certificate authorities, but

which also are experienced as logical and necessary to remain trust in the digital certificates. The burden of audits, but also the support for these audits is demonstrated by some quotes from the organizations that issue PKIoverheid certificates:

> Founder and CTO Digidentity: *"After the DigiNotar crisis the audits have become more stringent. Agentschap Telecom now does the inspection and that is appropriate. It has become harder for us, but we are engaged in serious matters and cannot allow mistakes. It is good that we are under inspection."* (personal interview, May 2, 2018: transcript S16)

> Commercial director QuoVadis: *"So not only by Logius, but in the new situation we have Agentschap Telecom as watchdog, so they are watching as well. We have the BSI-auditor and the eIDAS-auditor that check if you are compliant with the rules. You of course have other organisations that are asking questions, like: to what extent..? So the inspection of our type of organizations has increased and I only encourage that."* (personal interview, May 9, 2018: transcript S17)

> Compliance consultant KPN: *"You know it is part of it. It is more like that you now have let an independent organization establish what you are hoping for."* (personal interview, May 23, 2018: transcript S18)

When applying Whelan's (2011) framework to the current structure of the PKIoverheid system, we see that the power over the PKIoverheid system remains in the hands of Logius, who is still the hub in a network of contractual public-private partnerships. Internal network governance thus remains to be brokered. Regarding goal consensus, all parties are looking to issue secure digital certificates and to maintain the trust in public key infrastructures more than ever, as a new incident probably will be fatal for the PKIoverheid system. Provan and Kenis' (2008) lead organization-governed network therefore continues to be the model that most resembles the PKIoverheid system.

However, organizations like the European Commission and the CAB Forum have successfully imposed additional requirements and in that sense have gained power in the field of digital certificates services in general, but also in the PKIoverheid system. In that respect, these organizations have direct influence, but they are not part of the PKIoverheid system. Undisputedly, their presence is felt by the public and the private side of the arrangement.

4.3.3 Network culture

Before the DigiNotar crisis, flaws in security attention and risk awareness, and an overabundance of trust were recognized in the organizational culture of DigiNotar, Logius and OPTA. It were these characteristics that ultimately contributed to the crisis. However, other certificate authorities seemed well aware of the risks and of the importance of proper security measures, and also knew overreliance on trust was undesirable in the field of digital certificate services. This section will observe the same traits and will explore if cultural differences on these topics still exist.

During the interviews, it soon became apparent that risk awareness and security attention are on a much higher level since the DigiNotar crisis, and that the times of blind trust in other organizations are over. The main reason for this is quite simple. The PKIoverheid system most likely cannot afford another compromise of its certificates. The reputation of PKIoverheid suffered an immense blow at the DigiNotar crisis and the browser vendors have not forgotten this. If any incident like DigiNotar would happen again in the PKIoverheid system, the browsers will probably lose their faith in PKIoverheid indefinitely. Such could be the end of PKIoverheid as a public key infrastructure.

The sensitivity of this - and how this translates back to the organizational culture of the parties involved in PKIoverheid - is perhaps best illustrated by some extracts from the interviews:

> Policy authority Logius: *"The likes of QuoVadis, KPN, and Digidentity very well know that measures to maintain trust in the PKIoverheid system are necessary, as I will be held responsible by the browsers for any harm to the integrity of PKIoverheid certificates. If these browsers do not trust PKIoverheid anymore, websites with the PKIoverheid certificate will produce a red cross and that is very undesirable."* (personal interview, April 25, 2018: transcript C6)

> Founder and CTO Digidentity: *"If it happens again, the whole PKIoverheid system in the Netherlands will be in worldwide doubt. The browsers have not tightened the rules for nothing. I think that if it happens again, the whole PKIoverheid system might collapse."* (personal interview, May 2, 2018: transcript C7)

> Commercial QuoVadis: *"I think that whenever something similar happens again, with a different provider or with us, that not only the responsible provider, but the whole*

PKIoverheid system will be dropped. The CAB forum then will say: that small country over there.. and then we have a problem. They will not be able to determine if the end entity caused the issue or if the problem happened higher up in the chain. The CAB Forum will then drop the whole PKIoverheid system. Then we have a problem." (personal interview, May 9, 2018: transcript C8)

Coordinator Agentschap Telecom: "*DigiNotar has had major impact, not only on the sector here, but worldwide. I always say: DigiNotar made us world-famous in this sector. And that has led to or made that the people involved in this have become more aware. We cannot permit something like this to happen again. In addition, when we are abroad, as we have regular meetings with foreign watchdogs, DigiNotar always comes back. Always."* (personal interview, May 22, 2018, transcript C9)

The policy authority at Logius also added that raised security attention and risk awareness has not only been confined to the Netherlands, but that incidents with trust have raised such awareness worldwide. Certificate authorities will be held accountable for not being compliant with the valid norms and requirements, and it is very difficult to win back confidence once it has been lost. Pressure on this is so high, that all certificate providers are well aware of the importance of risk awareness, security attention, and trust (policy authority Logius, personal interview, April 25, 2018: transcript C10).

Raised security attention and risk awareness also started to better find their ways to the boardrooms. According to the senior official at the Ministry of Interior and Kingdom Relations, there was a bigger wave of cyber security awareness going on among policymakers after the DigiNotar crisis, but it is hard to fully attribute this to the DigiNotar crisis. The government's digitalization agenda, with cyber security high on it, was already present and continued to be pursued. This also played an important role in increased risk awareness. On the other hand, the DigiNotar crisis instigated sharpened norms, increased security awareness, and the strengthening of the network around PKIoverheid, which were all felt in the boardrooms (senior official MinBZK, personal interview, May 14, 2018: transcript C11).

To sum it all up, and as the senior official of the Ministry of Interior and Kingdom Relations expressed: within the PKIoverheid system there now is a feeling of togetherness and team spirit, and the shared idea that all parties involved do not want anything like the

DigiNotar crisis to happen again (senior official MinBZK, personal interview, May 14, 2018: transcript C12).

Looking through the lens of analytical framework, there now is a strong, shared culture with a focus on security attention and risk awareness. Such a culture is shared among the partners for the sake of the existence of the PKIoverheid system, leading to a form of cultural homogeneity. Solid membership over a long period of time, mutual interests, and a shared emotional experience in the form of the DigiNotar crisis have contributed to such a culture. This culture now seems to be well-rooted and should benefit the network effectiveness now and in the long-term.

4.3.4 Network policies

Policy within the PKIoverheid system and policy for digital certificates in general have significantly changed after the DigiNotar crisis, so has legislation. This section will first look into policy and legislation changes on national level, then on European level, and subsequently on worldwide level.

After the DigiNotar crisis, the Dutch House of Representatives immediately called for new legislation, particularly to enforce an obligation to quickly report security incidents. As new legislation takes time, policymakers at the Dutch Ministry of Interior and Kingdom Relations proposed self-regulation instead, because government organizations were willing to make changes themselves (senior official BZK, personal interview, May 14, 2018: transcript P3).

This solution fits in a broader perspective on the implementation of new legislation in the field of cyber security, in which self-regulation was preferred. New legislation is fine when it is convenient or when it protects involved parties, but it is not a goal (senior coordinating advisor NCSC, personal interview, May 1, 2018: transcript P4). Ultimately, the calls for legislation by the House of Representatives did result in the Data Processing and Cybersecurity Notification Obligation Act (Wgmc), which applies to cyber security incidents in public-private partnerships. Reporting has become obligatory since January 1, 2018, confirming that legislation indeed takes time (NCSC, 2017).

After DigiNotar, an also beyond the PKIoverheid system, information security became a policy priority at the Ministry of Interior and Kingdom Relations. Whereas information security first was arranged per division within the Ministry, now an overarching vision on information security was developed. Such a vision lined out security norms, crisis

plans, and risk analyses (senior official MinBZK, personal interview, May 14, 2018: transcript P5).

In the meanwhile, Logius remained the policy authority of PKIoverheid and was still responsible for the program of requirements, which was adjusted after the DigiNotar crisis. OPTA was still the oversight body that watched over the compliance with Dutch telecom law and thus over qualified certificates, until AT succeeded OPTA in 2012. Both parties were demanded to sharpen their norms and to become more stringent in oversight, resulting in company visits and more frequent audits. However, after 2015 the frequency of company visits and audits by Logius dropped, because additional requirements or legislation by other parties like the CAB Forum and the European Commission had led to an even more intensified burden of audit (policy authority Logius, personal interview, April 25, 2018: transcript P6).

On a European level, the 1999 European Commission directive for electronic signatures was succeeded by the eIDAS regulation, which was announced on July 23, 2014 and applied from July 1, 2016. The eIDAS regulation had to be implemented by all EU member states, resulting in changes to Dutch legislation. AT was appointed as watchdog over digital certificates and its authorizations were laid out in Dutch telecom law (coordinator AT, personal interview, May 22, 2018: transcript P7).

The eIDAS regulation is described in rather general terms, so to properly interpret the eIDAS regulation, more specific norms had to be formulated. ETSI became the preferred supplier for these norms. A certificate authority can also use different norm sets, but if a European certificate authority complies to the ETSI norms for digital certificates and electronic signatures, it simplifies the audits (coordinator AT, personal interview, May 22, 2018: transcript P8).

This burden of audits resulting from the eIDAS regulation was felt most by the certificate authorities and is best illustrated by an example. Before eIDAS, the certificate authorities could change its products or services without a preliminary audit. Auditing was done after the change was implemented, any adjustments deemed necessary by the auditor could be made later. After eIDAS, significant changes in products or services now had to be checked beforehand by the external auditor, which reported to AT. When AT green-lit the change, the certificate authority could start to implement it. This is experienced as affecting the flexibility of the certificate authority, but is perceived better in terms of risk (commercial director QuoVadis, personal interview, May 9, 2018: transcript P9).

Next to eIDAS, the browser vendors - by means of the CAB Forum - also imposed requirements to enhance the security standards of digital certificates, such as the Baseline Requirements for SSL certificates. These requirements were first published in 2011 - shortly after the DigiNotar crisis - and became effective in 2012. These requirements have been adjusted and updated since and force the certificate authorities to comply (CAB Forum, n.d.). If certificate authorities not comply, their certificates are refused by popular browsers like Microsoft Internet Explorer, Apple Safari, Google Chrome, and Mozilla Firefox. This practically means that their certificates become useless.

Some consequences of the increasing power of the CAB Forum are that SSL certificates are now valid for two years instead of three years, and that certificate authorities now first have to check if they are allowed to issue a certificate for a certain domain, as a registered company or user now can assign one specific certificate authority to be allowed to issue certificates for his domain (commercial director QuoVadis, personal interview May 9, 2018: transcript P10).

So, after the DigiNotar crisis, there is an enormous increase in rules and requirements that aim at minimizing risk and at maximizing security, all to maintain the trust in digital certificates and internet traffic. At national level, the influence on the requirements for digital certificates thus decreases and shifts to more international organizations like the European Commission and the CAB Forum. As a result, the increase in requirements resonates in multiple audits that check on ETSI norms, eIDAS regulation, CAB Forum requirements, Dutch telecom law, and Logius' program of requirements (commercial director QuoVadis, personal interview, May 9, 2018: transcript P11; policy authority Logius, personal interview, April 25, 2018: transcript P12).

Despite being a burden, the intensified audits are supported by the certificate authorities in the PKIoverheid system. Executives of certificate authorities said that the audits have become more stringent, making operations harder, but that these audits are necessary because of the seriousness of the business conducted at the company (founder and CTO Digidentity, personal interview, May 2, 2018: transcript P13); and that extra monitoring, even when the company thinks it is doing well, is necessary and that criticism can lead to improvements (commercial director QuoVadis, personal interview, May 9, 2018: transcript P14). These statements fit in the bigger picture of enhancing security and risk awareness, as discussed earlier in chapter 4.3.3.

When applying the analytical framework, in which Whelan (2011) argues that policy needs to be supported by culture, this is certainly true for the proliferation of rules,

requirements, legislation and policy. The certificate authorities, although they sometimes experience little flexibility, know what is at stake and therefore accept stringent rules and intensified oversight to minimize risk. Although most new norms were not developed at network level, their acceptance and their compliance has improved internal network control and stability in the PKIoverheid system.

4.3.5 Network technologies

The use of shared technologies among the partners within PKIoverheid has hardly changed. E-mail and phone calls are still the main technologies to communicate with each other. New forms of communication like WhatsApp are used as well, but there is no specific technology that has been designed to improve the effectiveness of PKIoverheid (senior official BZK, personal interview, May 14, 2018: transcript T5).

A key issue in using shared technologies or shared data in the field of digital certificates is that certificate authorities handle great amounts of personal data to establish who the applicants for certificates are. The General Data Protection Regulation (GDPR) now complicates sharing such information with other organizations. This means that the only thing that can be shared among the partners is publicly known information. For the exchange of publicly known information there is no necessity to use specific technologies, apart from e-mail (commercial director QuoVadis, personal interview, May 9, 2018: transcript T6).

However, Logius has developed a non-public log with PKIoverheid certificates, in which they can to keep track of PKIoverheid certificates issued by their partners (policy authority Logius, personal interview, April 25, 2018: transcript T7). Moreover, and outside of the PKIoverheid system, there now is an initiative called Certificate Transparency, in which Google plays a lead role. Certificate Transparency can be used to monitor, audit, or check if a digital certificate is used maliciously or has been issued falsely (Certificate Transparency, n.d.).

Everyone can access Certificate Transparency to see which certificates the Dutch certificate authorities have issued. So can, for example, Logius (consultant KPN, personal interview, May 23, 2018: transcript T8). Additionally Logius can consult their own log of PKIoverheid certificates. After the DigiNotar crisis, RAD and OVV criticized the lack of such databases. This hiatus is now filled.

Another technological development that came up during the interviews, again outside of the PKIoverheid network and not directly tied to digital certificates, is the rollout of a National Detection Network (NDN). NDN is a cooperation, guided by NCSC, in which

public and private parties invest in faster and improved observation and notification of digital threats and risks. By sharing this information, the parties can take measures to prevent or to restrict damage to their operations (senior coordinating advisor NCSC, personal interview. May 1, 2018: transcript T9).

Whilst on national level we see the first developments on shared technologies in cyber security public-private partnerships, the PKIoverheid system does not make use of shared technologies. The parties do not experience a necessity for such technologies, as e-mail suffices. Moreover, legislation like the GDPR obstructs the use of sharing detailed information about digital certificates. Shared technological infrastructure most likely does not exist, just as before the DigiNotar crisis, because it does not directly support the network goals. Databases that log issued digital certificates now do exist, but are either non-public in the case of Logius, or developed outside the PKIoverheid system in the case of Certificate Transparency.

4.3.6 Network relationships

Directly after the DigiNotar crisis, trust in the PKIoverheid system had come under pressure. This pertained not only to trust in the PKIoverheid certificates, but also concerned interorganizational trust, for example between the Ministry of Interior and Kingdom Relations and Logius. According to Whelan's (2011) framework, trust is important in environments of risk and trust helps to overcome problems. To increase the network effectiveness of the PKIoverheid system, trust thus had to be rebuilt.

Much interorganizational trust was rebuilt - or enforced - by changes in policy, by the increasing amount of audits, and by government oversight. The senior official at the Ministry of Interior and Kingdom Relations admits that confidence in Logius had been shaken, but it now has been fully restored because of Logius' sharpened oversight, their expertise, and their more emphatic role in the PKIoverheid system (senior official BZK, personal interview, May 14, 2018: transcript R6).

The senior official added that, largely in response to the DigiNotar crisis, informal relationships and trust was heavily invested in, and are extremely important. The relationships that were built, continue to exist and come in useful when new plans or activities are put forth, certainly when there is no legal basis to enforce these plans (senior official BZK, personal interview, May 14, 2018: transcript R7).

Agentschap Telecom, as the legally appointed oversight organization, handles relationships differently. The relationships are professional and are good working

relationships, for example when both AT and Logius visit a certificate authority for an audit. However, AT keeps its distance from other parties and has no informal contacts. This also goes for the relationships with the certificate authorities, who can consult AT for interpretation and explanation, but who also can be called to account by AT in case of anomalies. The main reasons for keeping relationships professional are to maintain legitimacy and authority as a watchdog (coordinator AT, personal interview, May 22, 2018: transcript R8).

When asking the certificate authorities about the role of relationships in the PKIoverheid system, these relations are experienced as good, but are mainly limited to the context of the PKIoverheid system:

> Commercial director QuoVadis: *"PKIoverheid is a small world. We know all the actors in the industry. You know who to get in touch with, because most of us are in this game for quite some years."* (personal interview, May 9, 2018: transcript R9)

> Founder and CTO of Digidentity: *"We are competitors, but we also want to keep the PKIoverheid system alive. Therefore, we have good relationships with QuoVadis and KPN. It is good to know each other, when there is a crisis you need each other."* (personal interview, May 2, 2018: transcript R10)

> Consultant KPN: *"When for example there are misunderstandings, it helps that you know someone. In that respect it is useful, but other than that.."* (personal interview, May 23, 2018: transcript R11)

Interpersonal trust and informal relationships thus do not seem to be affected that much by the DigiNotar crisis and remain good, but professional. Both can contribute to overcome problems and to enhance the network effectiveness. PKIoverheid continues to be a small world in which all parties know each other well and are clearly aware of their interdependence on each other. Interorganizational trust was restored as well, partly through oversight and intensified efforts to maintain relationships, but also partly out of the necessity to keep the PKIoverheid system alive and to guarantee the network's survival.

4.3.7 Subsidiary conclusion

This chapter has used the analytical framework to analyze the characteristics of public-private partnerships that operated in the PKIoverheid system the after the DigiNotar crisis. The analysis was mainly based on interviews with relevant stakeholders to best capture the developments in the years after the DigiNotar crisis.

The network structure remains characterized by brokered internal network governance. Logius, on behalf of the Ministry of Interior and Kingdom Relations, is the central hub of the network and exercises power through bilateral contracts and the program of requirements. In that sense, the network structure remained similar to Provan and Kenis' (2008) lead organization-governed model. Notable is the much larger influence of the European Commission and the CAB Forum, which both imposed additional norms and requirements for digital certificate services after the DigiNotar crisis.

The network culture has developed significantly. The DigiNotar crisis served as a learning experience and made all PKIoverheid parties more aware of the risks of insufficient security measures and failing oversight arrangements. Raised awareness is now central to the culture of the network and is shared among all participants, mostly because a new incident is expected to threaten the existence of PKIoverheid as a public key infrastructure. Therefore, the shared culture is crucial for the network to operate effectively.

After the DigiNotar crisis, norm sets and regulation for digital certificates proliferated and were largely imposed from outside the PKIoverheid system, leading to an increased amount of audits. This also resonated in the network policies of the PKIoverheid system, as the eIDAS regulation forced changes in Dutch legislation and the CAB Forum requirements were implemented in Logius' program of requirements. The growing number of rules, norms, and regulations was established to minimize risk and to enhance control over digital certificate services. The audits and the absence of large incidents in the PKIoverheid system prove that these policies have managed risk rather successfully.

The shared network technologies are restricted to e-mail, phone calls, and communication through WhatsApp. The network participants do not experience the need for shared technological infrastructure, which also might prove to be problematic due to GDPR restrictions on sharing data. Logius now runs a non-public log for PKIoverheid certificates and the international initiative Certificate Transparency gives insight to PKIoverheid and other digital certificates as well, but was developed outside the PKIoverheid system. Also beyond the PKIoverheid system, NCSC managed the development of a public-private national detection network for quick observation and assessment of cyber threats.

The network relationships are crucial in overcoming problems or for creating support for new plans. Interpersonal relations, formal or informal, were hardly affected. Interorganizational trust was slowly restored after successful audits and sharpening of norms and oversight. Trust and good relationships are also largely influenced by the interdependence of the network participants and the shared goal to keep the PKIoverheid system alive.

Conclusively, the DigiNotar crisis forced PKIoverheid stakeholders to rethink or to remodel, and led to significant changes in culture, policies, and relationships. However, the interviews also suggest that the influence of the DigiNotar must not be overstated, as the government's digitalization agenda also gave rise to broad cyber security awareness among policymakers and politicians, and the development of new cyber security legislation and initiatives.

4.4 Conclusion

Now the thesis' sub questions have been answered, this section will summarize the main findings of this study and will address the main research question: *To what extent has the DigiNotar crisis changed the characteristics of public-private partnerships in the PKIoverheid system, and how can this be explained*?

After providing a short summary of the DigiNotar crisis, this section will compare the characteristics of public-private partnerships before and after the DigiNotar crisis, and will look for explanations for changes in these characteristics. The conclusion will be drawn in accordance to the analytical framework that was presented in chapter 2.3.1.

4.4.1 The DigiNotar crisis

The DigiNotar crisis was a landmark moment in the still young history of the Dutch cyber security sector. A hack at private certificate authority DigiNotar led to the issuance of hundreds of rogue digital certificates, of which one certificate was suspected to be used to intercept information of Iranian Gmail-users, for which the direct consequences remain unclear, but may have been fatal. The DigiNotar crisis exposed weak security precautions and low risk awareness at the company of DigiNotar, but it also exposed failing oversight by Dutch government agencies Logius and OPTA.

The DigiNotar crisis served as a wake-up call for the Dutch government, which realized it had to step up its game in securing the digital certificates of the PKIoverheid system, which were key ingredients for secure and trustworthy internet communication between a wide array of internet users, ranging from governments to citizens to businesses. After the DigiNotar crisis, the Dutch government announced a number of measures to prevent a similar crisis from ever happening again. The aim of the study was to see if public-private arrangements in the PKIoverheid system indeed have changed.

4.4.2 Differences in the characteristics of public-private partnerships

The study used Whelan's (2011) framework for network dynamics and network effectiveness to study five levels of analysis: network structure, network culture, network policies, network technologies, and network relationships. This framework was complemented with ideas from Provan and Kenis (2008) and Kenis and Provan (2009) on network structure, and ideas from Jahner and Krcmar (2005) on network culture.

4.4.2.1 Network structure

The study found that the network structure resembled the form of a hub, with government agency Logius as the lead organization that governed the network of public-private partnerships that provided PKIoverheid certificates. Logius held power through contracts with the private certificate authorities. This remained unchanged after the crisis, as the PKIoverheid system remained a responsibility of the Dutch Ministry of Interior and Kingdom Relations, which regained trust in Logius after oversight arrangements were changed and new norms were complied with successfully.

However, organizations like the European Commission and browsers vendors, by means of the Certificate Authority/Browser Forum, became increasingly influential by imposing new legislation and requirements that certificate authorities had to abide by to remain trusted partners. Both organizations made these efforts to improve the trustworthiness of digital certificates in particular, and internet communication as a whole. Although powerful, these organizations are not part of the PKIoverheid system.

4.4.2.2 Network culture

Studying the network culture of the PKIoverheid system brought to light that, before the DigiNotar crisis, a lack of security attention and risk awareness were at the heart of failing security precautions at DigiNotar, almost facilitating hacker access. Such a lack of security attention and risk awareness was also found at Logius and OPTA, who confided too much in the audit reports of the accredited auditor, which only checked for compliance with an incomprehensive norm set. Based on the interviews, such a feeble risk culture was not found at other private certificate authorities, but these cultural differences only came to light when the damage was done.

The interviews learned that the DigiNotar crisis had led to significant change in the network culture, as all organizations involved in the PKIoverheid system now are well aware of the risks of weak security precautions and lacking oversight. Increased risk awareness also goes beyond the PKIoverheid, as it led to a better understanding of risks and increased alertness in the Dutch cyber security sector in general, and that it led to the topic of cyber security reaching the boardrooms.

For the PKIoverheid system changes are easy to explain: a new compromise of the PKIoverheid will most likely lead to the revocation of trust by the increasingly more powerful browsers vendors, meaning the end of the PKIoverheid system. This forces the members of PKIoverheid to adapt. For the Dutch cyber security sector in general, a larger

trend of digitalization also played part in increased awareness, but it can hardly be considered a coincidence that this wave of awareness gained momentum in the aftermath of the DigiNotar crisis.

4.4.2.3 Network policies

When comparing the network policies designed to enhance internal network control, the program of requirements of Logius still exists, but has implemented changes that are rooted in newly imposed requirements by the CAB Forum and the European Commission in the form of the Baseline Requirements and the eIDAS regulation. The eIDAS regulation also forced changes to Dutch telecom law, which appointed Agentschap Telecom as national watchdog.

The enforcement of these requirements was exercised through more stringent oversight by Logius and by AT, that had started to regularly visit the certificate authorities for inspections. Together with visits from independent auditors this led to a significantly increased burden of audits, that checked on Logius' program of requirements, ETSI norms, eIDAS regulation, and CAB Forum requirements.

Changes due to the eIDAS regulation can be seen in the light of increasing involvement of the European Commission in national affairs. Implementation of CAB Forum requirements can be explained by the increasing power of the browser vendors, which practically maintain a policy of comply-or-die to protect its users.

On a national level, cyber security became a policy priority due to the increased security awareness. Additionally, legislation on obligatory reporting of security breaches, which the House of Representatives called for directly after the DigiNotar crisis, came into force as of January 1, 2018. This legislation process was initiated after the DigiNotar crisis, but had taken due time.

4.4.2.4 Network technologies

Both before and after the DigiNotar crisis the organizations of the PKIoverheid systems did or do not use shared network technologies. This can be explained by the lack of a necessity for such technologies. The GDPR complicates shared databases about certificates, and the exchange of publicly known information or personal communications is done by phone, e-mail, or more recent technologies like WhatsApp.

PKIoverheid certificates are now logged by Logius and can be found through the Certificate Transparency initiative. However, Logius' PKIoverheid log is non-public and the

Certificate Transparency initiative was developed outside the PKIoverheid systems and concerns digital certificates worldwide. These databases do fill the hiatus that RAD and OVV identified and can smoothen the substitution of compromised certificates in case of a new breach.

4.4.2.5 Network relationships

Interpersonal relationships were generally perceived as crucial for overcoming problems, before and after the DigiNotar crisis. The degree of formality differs as AT en Logius require legitimacy and authority, but informal relationships are considered to sometimes be more effective than formal procedures. The small world of PKIoverheid strongly determines these interpersonal relationships.

After the DigiNotar interorganizational trust had eroded, in particular between the Ministry of Interior and Kingdom Relations and government agency Logius. That interorganizational trust between the PKIoverheid stakeholders now has been rebuilt, which can be best explained by the interdependence on each other's organizations to keep the PKIoverheid system alive, but also because of successful audit and oversight.

4.4.2.6 General conclusion

The DigiNotar crisis led to significant changes in the characteristics of public-private partnerships in the PKIoverheid system, in particular with regard to culture, policies and relationships. Currently, the public-private partnerships in the PKIoverheid system appear to be sound arrangements, in which security attention and risk awareness have become important values. The shared interest to keep the PKIoverheid is the main incentive and in that respect, the organizations of PKIoverheid are all on the same page, with a shared situational awareness that is beneficial to the network effectiveness.

These changes in the characteristics of the public-private partnerships in the PKIoverheid system should prevent a breach similar to that of DigiNotar to happen again. However, with malicious adversaries becoming increasingly more advanced, such a statement might be a little too bold. Therefore, it remains of utmost importance to uphold security standards and to report security breaches.

Lastly, the DigiNotar crisis also had effects beyond the PKIoverheid system, increasing security and risk awareness among policymakers and boardroom executives in the Netherlands. On the other hand, this influence must also not be overstated, as the

digitalization of the Dutch government was in full swing in the periods surrounding the DigiNotar crisis.

5. Reflection

This chapter looks back on the research. The next paragraphs discuss the limitations of the study, the study's contribution to science, and the study's contribution to society. The thesis is concluded with recommendations for policy and recommendations for further study.

5.1 Discussion of limitations

One of the main limitations of this study is that it reflects only a small amount of opinions of PKIoverheid stakeholders. Although both public and private have been heard extensively, opinions on the characteristics of public-private partnerships might change per organizational level. This study has mainly heard executives or senior level employees, almost all of them longstanding members of the PKIoverheid system. Newcomers in this system might judge otherwise on the changes in the public-private partnerships that constitute the PKIoverheid system.

On the other hand, it was a privilege to talk to stakeholders with a long record of experience in the PKIoverheid system, as they proved to give interesting and very specific insights in historical, but also in recent developments of all aspects of the PKIoverheid system. I therefore find it hard to speak of the limited scope of interviewees as a real limitation, as the data from the interviews is the backbone of this thesis, which could not be written without.

Furthermore, the original objective of this thesis was to study changes in the characteristics of public-private partnerships in the Dutch cyber security sector in general. Yet, whilst collecting the data it soon became apparent that many public-private partnerships - particularly in a broad and still expanding domain like that of cyber security - are tailored to the sector in which the partnership operates or to what product has to be delivered. Therefore, I chose to specifically focus on public-private partnerships that operate in the PKIoverheid system.

This choice might limit the generalizability of the study's results to the broader Dutch cyber security sector, but it allowed for a better systematic analysis of the public-private partnerships that most felt the effects of the DigiNotar crisis. Still, as the interviews and the analysis of data eventually suggested, a broader effect of increased risk awareness in the Dutch cyber security after the DigiNotar crisis was perceived. However, the true effect is hard to measure, as on-going digital developments blur the lines between the causal factors.

5.2 Contribution to science and society

I believe it is fair to say that the description of the DigiNotar crisis and the analysis of the characteristics of public-private partnerships in the PKIoverheid system before the DigiNotar crisis are hardly a groundbreaking effort. Whilst these chapters have brought together the perspectives of a range of different sources, it is the analysis of the current characteristics of public-private partnerships in the PKIoverheid system that breaks new ground.

Whilst studying public-private partnerships in the PKIoverheid system, this thesis has shown that Whelan's (2011) theory on network dynamics and network effectiveness, originally designed for networks in the national security sector, can also be applied when studying public-private partnerships in the cyber security sector.

Furthermore, the DigiNotar crisis and its direct aftermath drew worldwide attention, but almost no efforts - academic nor journalistic - have been dedicated to study the current arrangements of a sector so crucial to our trust in the internet, in the government, and in the digital services that are part of our daily life.

This is unfortunate, as still few people know about the indispensable role that digital certificates play in today's society. Digital identity will become increasingly more important, in the very near and in the distant future. Writing a thesis on this topic might contribute to a better appreciation of this field of expertise, albeit just slightly.

5.3 Recommendations for policy

Although this thesis has established that arrangements in the PKIoverheid have changed positively, there are always improvements that can be made. Something that stood out during the interviews were the different interpretations of the concept public-private partnership. The public organizations saw PKIoverheid more as a partnership than the private organizations did. The private certificate authorities considered the arrangement between public and private to be more unilateral than bilateral.

On the one hand - and with the DigiNotar crisis still in mind - such a strong lead by the public organizations seems logical, as they are ultimately responsible for the PKIoverheid system. On the other hand, a more democratic partnership might contribute to a better overall feeling about the partnership by all its participants, which in turn can benefit the effectiveness of the PKIoverheid system even more. Although consensus is often striven for, there are still gains to be made here.

Another recommendation for policy would be increased uniformity of norms and requirements for the issuance of digital certificates, as a variety of organizations now impose

requirements on certificate authorities for different types of digital certificates. Although efforts to alleviate the burden of audit are currently on-going, a certificate authority still has to welcome multiple auditors that check on different sets of norms. Increased uniformity of norms and requirements might change this for the better. However, increased uniformity will require international efforts and the willingness of powerful organizations like the European Commission and large American corporations that cherish that their sovereignty.

A recommendation that is a bit wilder, is to reconsider the necessity of the PKIoverheid system as a whole, now the requirements imposed by the European Commission, ETSI, and the CAB Forum have already created very strict rules for the issuance of digital certificates, and many of these rules haven been implemented by Logius into their program of requirements. In this scenario, certificate authorities could issue digital certificates that are not accredited by Dutch government, but do comply with all other important requirements for digital certificates and electronic signatures. Logius could then leave oversight to AT and focus on the other digital services they provide.

Yet, such a scenario might also be problematic, as many digital certificates have to be substituted in due time, which then might threaten the continuity of critical government and non-government, as we have seen during the DigiNotar crisis. I also find it hard to say what other consequences might follow from such a scenario and whether this will have a positive or a negative impact on the organizations that are part of the PKIoverheid system.

5.4 Recommendations for further study

Regarding recommendations for further study, I see added value in a more technical analysis of how the public key infrastructure of PKIoverheid has changed after the DigiNotar crisis, as now - roughly seven years after the DigiNotar crisis - adversaries have become more advanced, technical security standards have become higher, and additional technical requirements have been imposed by the likes of the European Commission and the CAB Forum. Such a technical study was beyond the scope of this, but would contribute to painting a bigger and better picture of the technological consequences of the DigiNotar crisis.

Another interesting avenue for further research would be to study other European government owned public key infrastructures and how other European governments cope with eIDAS regulation, CAB Forum, and oversight. During this thesis, it was hard to get a better picture of such arrangements and it was difficult to establish if the PKIoverheid system is unique or quite generic. However, his would call for a broad, European approach, also outside the range of this thesis.

Bibliography

ACM. (2011, October 3). Fusie van CA, NMa en OpTA per 1 januari 2013 voorzien. *ACM*. Retrieved from https://www.acm.nl/nl/publicaties/publicatie/7469/Fusie-van-CA-NMa-en-OPTA-per-1-januari-2013-voorzien.

Agentschap Telecom. (2017). *Samenwerkingsprotocol Logius - Agentschap Telecom.* Retrieved from https://www.agentschaptelecom.nl/documenten/publicaties/2018/februari/16/samenwerkingsprotocol-logius.

Alibo. (2011, August 27). Is this MITM attack on SSL's certificate? *Google Help Forum*. Message posted to http://www.google.co.uk/support/forum/p/gmail/thread?tid=2da6158b094b225a&hl=en.

Boersma, K., Wagenaar, P., & Wolbers, J. Negotiating the 'Trading Zone'. Creating a Shared Information Infrastructure in the Dutch Public Safety Sector. *Journal of Homeland Security and Emergency Management, 9(2),* 1-25.

Boon, L. (2011, September 20). DigiNotar failliet verklaard. *NRC*. Retrieved from https://www.nrc.nl/nieuws/2011/09/20/diginotar-failliet-verklaard-a1452676.

Bryman, A. (2012). *Social Research Methods* (4th Ed.). Oxford: Oxford University Press.

CA/Browser Forum. (n.d.). Baseline Requirements Documents. *CA/Browser Forum*. Retrieved from https://cabforum.org/baseline-requirements-documents/.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs, 91(1),* 43-62.

Certificate Transparency. (n.d.). What is Certificate Transparency? *Certificate Transparency*. Retrieved from http://www.certificate-transparency.org/what-is-ct.

De Jongh, H. (2007, June 8). Virtuele notaris dankt de fiscus hartelijk; Bedrijfsportret van DigiNotar, een onderneming die goed geld verdient aan de bureaucratie. *Het Financieele Dagblad.* Retrieved from LexisNexis Academic.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics, 20(3),* 701-715.

Fox-IT. (2011). *Interim Report: DigiNotar Certificate Authority Breach "Operation Black Tulip".* Delft: Fox-IT.

Fox-IT. (2012). *Black Tulip: Report of the investigation into the DigiNotar Certificate Authority breach.* Delft: Fox-IT.

Hoogenboom, B.A. (1994). *Het politiecomplex*. Arnhem: Gouda Quint B.V.

Jahner, S., & Krcmar, H. (2005). Beyond technical aspects of information security: Risk culture as a success factor for IT risk management. *AMCIS 2005 Proceedings, paper 462,* 3327-3336.

Kenis, P., & Provan, K. G. (2009). Towards an exogenous theory of public network performance. *Public Administration, 87(3),* 440-456.

Klijn, E. H., & Teisman, G. R. (2003). Institutional and Strategic Barriers to Public-Private Partnership: An Analysis of Dutch Cases. *Public Money and Management, 23(3),* 137-146.

Kurapati, S., Kolfschoten, G., Verbraeck, A., Drachsler, H., Specht, M., & Brazier, F. (2012). A Theoretical Framework for Shared Situational Awareness in Sociotechnical Systems. In *Proceedings of the 2nd Workshop on Awareness and Reflection in Technology-Enhanced Learning (ARTEL 2012),* 47-53.

Linder, S. H. (1999). Coming to Terms with the Public-Private Partnership. *American Behavioral Scientist, 43(1),* 35-51.

Logica Business Consulting. (2012). *Evaluatie PKI: Rapportage*. Amstelveen: Logica Business Consulting.

Logius. (n.d.). PKIoverheid Certificaten. *Logius.* Retrieved from https://cert.pkioverheid.nl/.

Logius. (2017). *Certificate Practice Statement (CPS).* Den Haag: Logius.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures, 9(1-2),* 3-31.

Martin, Z. (2011, January 12). VASCO buys Netherlands' DigiNotar. *SecureIDNews.* Retrieved from https://www.secureidnews.com/news-item/vasco-buys-netherlands-diginotar/.

Maurer, U. (1996). Modelling a public-key infrastructure. In *European Symposium on Research in Computer Security,* 325-350. Berlin, Heidelberg: Springer.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2012a). Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties. *Kamerstukken II 2012-2013, 26643, 222.*

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2012b). Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties. *Kamerstukken II 2012-2013, 26643, 230.*

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2012c). Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties. *Kamerstukken II 2012-2013, 26643, 256.*

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2012d). Brief aan de voorzitter van de Onderzoeksraad voor de Veiligheid met reactie op het onderzoeksrapport inzake "Het DigiNotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt". *Kamerstukken II 2012-2013, 26643, 257.*

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Ministerie van Veiligheid en Justitie (2011a). Brief van de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van de Minister van Veiligheid en Justitie. *Kamerstukken II 2010-2011, 26643, 188.*

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Ministerie van Veiligheid en Justitie. (2011b). Brief van de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie. *Kamerstukken II 2010-2011, 26643, 189.*

NCSC. (2012, January 2). Nationaal Cyber Security Centrum (NCSC) bundelt kennis en expertise. *NCSC.* Retrieved from https://www.ncsc.nl/actueel/nieuwsberichten/nationaal-cyber-security-centrum-ncsc-bundelt-kennis-en-expertise.html.

NCSC. (2017, December 15). Wet gegevensverwerking en meldplicht cybersecurity. *NCSC.* Retrieved from https://www.ncsc.nl/actueel/nieuwsberichten/wet-gegevensverwerking-en-meldplicht-cybersecurity.html.

NCTV. (2011). *Nationale Cyber Security Strategie*. Den Haag: NCTV.

NCTV. (2013). *Nationale Cyber Security Strategie 2*. Den Haag: NCTV.

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches* (7th Ed.). Harlow: Pearson Educated Limited.

NOS. (2011, September 4). CIA, Mossad, providers doelwit hack. *NOS.* Retrieved from https://nos.nl/artikel/269899-cia-mossad-providers-doelwit-hack.html.

Onderzoeksraad voor Veiligheid. (2012). *Het DigiNotarincident: Waarom digitale veiligheid de bestuurstafel te weinig bereikt.* Den Haag: Onderzoeksraad voor Veiligheid.

Provan, K. G., & Kenis, P. (2008). Modes of Network Governance: Structure, Management, and Effectiveness. *Journal of public administration research and theory, 18(2),* 229-252.

Rijksauditdienst. (2012). *De zaak 'DigiNotar': handelde de overheid adequaat? Onderzoek naar alertheid en adequaatheid van handelen van de overheid ten tijde van de 'DigiNotar'-problematiek.* Den Haag: Rijksauditdienst.

Sørensen, E., & Torfing, J. (2005). The Democratic Anchorage of Networks. *Scandinavian Political Studies, 28(3),* 195-218.

Van der Kolk, T. (2011, August 30). Nederlandse overheidssites dupe van Iraanse hack. *De Volkskrant.* Retrieved from https://www.volkskrant.nl/vk/nl/2694/Internet-Media/article/detail/2877061/2011/08/30/Firefox-bestempelt-DigiD-als-onbetrouwbaar.dhtml.

Van der Kolk, T. (2011, August 8). Oud-eigenaren DigiNotar moeten vele miljoenen betalen. *De Volkskrant.* Retrieved from https://www.volkskrant.nl/media/oud-eigenaren-diginotar-moeten-vele-miljoenen-betalen~a3715499/.

Van der Meulen, N. (2013). DigiNotar: Dissecting the First Dutch Digital Disaster. *Journal of Strategic Security, 6(2),* 46-58.

Wettenhall, R. (2003). The Rhetoric and Reality of Public-Private Partnerships. *Public Organization Review: A Global Journal, 3,* 77-107.

Wetenschappelijke Raad voor het Regeringsbeleid. (2011). *iOverheid: Synopsis van WRR-rapport 86*. Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid.

Whelan, C. (2011). Network Dynamics and Network Effectiveness: A Methodological Framework for Public Sector Networks in the Field of National Security. *The Australian Journal of Public Administration, 70(3),* 275-286.

Wolff, J. (2016, December 21). How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure. *Slate.* Retrieved from http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_diginotar_changed_the_internet_s_infrastructure.html.

Zetter, K. (2011, September 20). DigiNotar Files for Bankruptcy in Wake of Devastating Hack. *Wired.* Retrieved from https://www.wired.com/2011/09/diginotar-bankruptcy/.