Policy instruments and the adoption of DNSSEC

A case study regarding the (semi-) public sector and Internet service providers.

Executive master's programme cyber security
Thesis René Bakker
Student number: S1789805
First reader: Dr. E. Erdemoglu
Second reader: Prof. dr. M.J.G. van Eeten

January 2018

Preface

The thesis presented here is to finish the program Executive Master Cyber Security, as organized by Leiden University, Delft University of Technology and The Hague University of Applied Science. One of the characteristics of this program is the multidisciplinary nature. Many cyber security issues include not only technical, but also economical or juridical questions. This is also the case with the casus discussed in this thesis. Although technical in nature, questions raised by adopting the Internet security standards like DNSSEC are quite different. But design essentials of the DNS determine what can and cannot be regulated. As Laurence Lessig put it, regulability is a function of design. In my opinion, multi-angled problems are characteristic for many challenges society faces in the digital age.

René Bakker

The Hague, 9 January 2018

Abstract

The rise of Internet and accompanying applications has provided immense opportunities for all kinds of businesses. The heart of the success of the Internet is its radically decentralized structure. The Domain Name System creates hierarchical domain names, that can be extended in a nearly infinite way. The DNS plays a central role in connecting numbers (IP addresses) to (domain) names, just as the phone book.

At the same time, we are increasingly harassed by security incidents. The DNS is important for the safety of e-mail (National Cyber Security Centre, 2015), relevant for phishing. By adding a digital signature to the DNS (DNSSEC), authentication of the source and integrity of the data can be provided. Since there are many ways to conduct phishing without abusing the DNS, it is hard to determine the exact impact of missing DNSSEC. Nevertheless, policymakers have designed a policy to increase the adoption of DNSSEC.

Recent research shows huge differences in the adoption of DNSSEC. In the (semi) public sector 59% of all domain names are DNSSEC signed, a rather high percentage. In the ISP sector around 22% of all companies use a signed domain. This raises the question how these differences can be explained. To do this the regulation of these sectors is considered. This is done by an explorative case study, that includes conducting interviews with most important actors in providing DNSSEC, and representatives of the sectors.

There are two key factors in providing a DNSSEC solution to the end-user. Hosting companies (including registrars) provide registrants with a DNSSEC signed domain name. Around 49% of all .nl domain names are DNSSEC signed, a rather high percentage. Equally important are access providers, who validate DNSSEC answers for their customers. This is done in around 22% of all DNS queries. This rather low percentage is partly due to the (perceived) complexity of DNSSEC adoption, information asymmetry and misaligned incentives. Also, in the case of large access providers investment costs are considerable (€ 200 – 300 k).

The adoption of DNSSEC in the (semi-) public sector is due to the comply-or-explain policy quite well incorporated. This is done by addressing responsibilities for architects, buying sections, and in audits. The (semi-) public sector tends to be risk avoiding. This explains the relatively high number of DNSSEC signed domain names in this sector. The Wet GDI is designed to take this policy one step further by introducing an obligation. A risk based approach as is common in cyber security guidelines and addressing limited validation of DNSSEC is missed here.

ISPs are not within scope of the comply-or-explain policy, nor of the Wet GDI. Also, risks are generally considered lower for ISPs than for the (semi-) public sector. It is economically rational to accept some insecurity, also because of the lack of DNS related incidents. In some cases, there are additional costs for a hosting ISP to adjust (open source) software to be able to use it for their own networks. These factors all together explain why only 22% of the ISPs use DNSSEC for securing their own domain name.

Best option to increase DNSSEC adoption for the policy maker is co-regulation. ISPs are in a good position to invest in cyber security, but because of public good characteristics and market failures they cannot do this on their own. Several examples show that information asymmetry can be corrected in different ways. (Co)-Financing and increasing public awareness can be promising to fight negative externalities and information asymmetries.

Table of content

Introduction

One of the main reasons for the success of the Internet is its radically decentralised structure. To communicate on the Internet every system needs a unique numeric Internet Protocol (IP) address. Since it is difficult for end-users to remember a long series of numbers, IP addresses are translated into names. This is the fundamental task of the Domain Name Server (DNS), that route messages around the network. This function is often compared with a 'phone book' for the Internet. (Post and Kehl 2014; 3)

Instead of maintaining telephone book, a system was designed, based on hierarchical domain names. This system allows levels to be added to the top-level domains (such as .com, .nl, .edu). So, a second level microsoft.com can be added, a third info.microsoft.com, and subsequently more. Owning a proper domain name (mostly the company name) is crucial for companies and other (semi-) public institutions.[1] By using hierarchical domain names, a nearly infinite growth is possible, that represents immense commercial and communicational value.

However, this decentralised system also comes with vulnerabilities. If the DNS is corrupt (for instance done by 'cache poisoning'), the end-user can be directed to a malicious website. This can be risky when sensitive (personal) information is exchanged, or a financial transaction is done. To counter this risk the Internet Engineering Task Force (IETF) adopted a solution to develop a secure version of the DNS. Two functions are added, authenticity to guarantee the legitimation of the source, and integrity to assure that data have not been altered. This is done by Domain Name System Security Extensions (DNSSEC), that make it possible to add a cryptographic signature to the domain.

There are two key factors in providing a DNSSEC solution to the end-user. On the one hand, an individual or a company (registrant) must be able to get a DNSSEC signed domain, including DNSSEC enabled hosting. This is provided to him by a *registrar*, that is usually also the *hosting provider*. It is also possible that DNS records are hosted by privately-owned DNS servers. On the other hand, DNS resolvers must present validated DNS answers to the end-user. This typically occurs on the infrastructure of another type of ISP, the *access provider*. It is important to note the difference between these two types of ISPs, because the incentives connected to adopting DNSSEC are quite different.

The top-level .nl domain is maintained by the Stichting Internet Domeinregistratie (SIDN). The DNSSEC solution became available in the Netherland when SIDN signed the top-level domain name with a cryptographic signature in 2010. This made it possible for registrars to issue domain names with cryptographic signatures for their customers. SIDN started an incentive program to encourage registrars to implement DNSSEC.

Initially this was quite successful and the number of DNSSEC signed domain names rose fairly quickly to approximately 25% at the end of 2012 (SIDN 2017; 5). But after this initial growth the pace of implementation declined. Recent figures show that around 49% of all Dutch domain names are DNSSEC signed("SIDN.nl stats and data," 2017)[2]. Since validation is equally important, the number of DNS

[1] Visitors will use this name while searching the Internet and the domain name is important for Google to list the results.

[2] From a global perspective this is relatively high. Worldwide adoption of DNSSEC is around 2% (Centraal Plan Bureau 2016, 23).

resolvers that support DNSSEC are also of interest. At the moment, about 22% of the DNS request in the Netherlands are DNSSEC validated. (APNIC, 2017a)

Recent research of the SIDN points out that there are differences in adopting DNSSEC for domain names between several sectors in the Netherlands. Within the (semi-) public sector 59% of the websites uses DNSSEC, which is relatively many. Where (semi-) public institutions only used in 11% signed domains in 2014, this raised to 59% in 2017. Especially municipalities are doing well. The number of signed domains rose from near to zero in 2014 to 63% in 2017. (SIDN; 19)

Within the telecom branch the use of DNSSEC is modest (33%), and this is also the case with Internet providers (22%).(SIDN 2017, 13). Only a limited number of large ISPs have signed their domain name. None of the big telecom operators (KPN, T-Mobile, Vodafone Libertel) have DNSSEC signed domain names. This while on average is 49% signed (DNSSEC, 2017c), a distinctive difference. Since ISPs are key in providing the DNSSEC, this is significant. To some extent the difference can be explained by the in general more sensitive services the (semi-) public sector offers, but as will be demonstrated this is not the only factor.

The variance in adoption levels of DNSSEC is the subject of this thesis[3]. What actors provide the DNSSEC solutions and what explanations can be found for the variance? The research focusses on the adoption of signed domains by (semi-) public institutions[4] and ISPs. In the research we will investigate what factors influence the adoption of DNSSEC. Since one missing part in the chain diminishes advantages, it is important that all actors are included.

According to the Cabinet, the limited adoption of DNSSEC signed domain names is a point of concern. ICT is a prerequisite for the Dutch economy. The Cabinet wishes to position the Dutch digital infrastructure as a third main port, next to Schiphol and the harbour of Rotterdam. In this reasoning, security of the infrastructure is a point of national interest. 'Safeguarding digital security and maintaining an open and innovative digital domain are preconditions for the proper functioning of our society' (National Cyber Security Strategy 2; 3). According to the policymakers, (semi-) public institutions should adopt Internet security standards like DNSSEC.

DNSSEC (and the other protocols) are standards that the department of Economic Affairs has added to the comply-or-explain list, coordinated by the Forum Standaardisatie. (Semi-) public authorities are required to use this list, unless there are very good reasons not to do so. [5] To encourage safer email services several parties guided by the department of Economic Affairs signed an agreement called the *Veilige e-mail coalitie.* Because of the role of the DNS in securing e-mail, the adoption of DNSSEC is part of the agreement.

[3] There are many examples of cyber (security) solutions, that are slowly implemented. Some of these techniques contribute to the scalability of the Internet (IPv6), while others increase safety (DMARC, SPF). Less than half of the government websites (44%) use a secure connection (NRC Handelsblad, 2017). Google statistics show IPv6 availability of approximately 18% amongst its users (Google, 2017)

[4] Since previous research of the SIDN has been used, the same definition as listed in this report will be used. The (semi-)public sector includes political organisations, governmental organisations, municipalities, zbo's, enforcement agencies, care institutions, and higher educational institutions. (SIDN, 2017d).

[5] For this reason, the Department of General Affairs, that registers central domain names for the government, shuts down e-mail functionalities when a domain is issued. This functionally will only be available if all standards required for e-mail are adopted. ("'Tandje erbij met e-mailbeveiliging overheid' - Binnenlands Bestuur," 2017)

In a recent letter to the Parliament Minister Kamp emphasises the importance of Internet security standards like DNSSEC (Ministerie van Economische Zaken, 2017a). According to Kamp, the standards enhance the safe exchange of information and are a prerequisite for the exchange of information between companies, civilians, and the (semi-) public authorities. In the letter Minister Kamp expresses his concern about the slow pace of adoption of Internet security standards like DNSSEC within the (semi-) public sector. (Ministerie van Economische Zaken 2017; 1)

According to the Cabinet, the pace of adopting DNSSEC signed domain names is too slow. For this reason, an obligation is designed for public authorities to adopt Internet security standards (including DNSSEC)[6]. This obligation is formulated in the Wet generieke digitale infrastructuur (Wet GDI[7]), that stipulates conditions that make this necessary. The proposal consists of a rule to introduce Internet security standards by *Algemene Maatregel van Bestuur*, so it can be established by a minister without consulting the parliament. This makes it easier and faster to add (or remove) required standards. (Ministerie van Binnenlandse Zaken, 2017a)

Relevant goals of the Wet GDI are:

- To make Internet security standards for (semi-) public authorities an obligation;
- To increase safety, reliability and working of digital services;
- To increase trust within society in digital services amongst citizens and entrepreneurs. (Ministerie van Binnenlandse Zaken 2017; 3)

In this thesis, we will investigate what factors influence the adoption of DNSSEC. This will include actors and incentives to adopt it. Introducing new technology requires investments in infrastructure, education, and software. The adoption of DNSSEC is of interest to increase the security of e-mail, but also requires investments of several actors. Decisions to invest in increasing security are based on a balanced outcome of pros and cons, the return-on-investment.

For policy makers, an analysis of all players and (misaligned) incentives can prove helpful to abate impediments that hamper the implementation of DNSSEC. At the moment, there is no overview of all stakeholders and necessary investments in the Dutch situation[8]. Without such overview, it is very difficult to design a public policy. Existing regulation in the (semi-) public sector and in the ISP branch is investigated. Part of the research is an assessment of the effectiveness of the regime and the (expected) Wet GDI.

[6] Currently in preparation, draft reviewed after public consultation. (Ministerie van Binnenlandse Zaken, 2017b)
[7] Recently renamed in *wet Digitale Overheid.*
[8] On a European level a research on this topic is published some years ago, see for this Enisa report, the costs of DNSSEC deployment (Enisia, 2012). Also very recently on November 3 2017 an article is published about the role of registrars, where DNSSEC deployment is studied in detail. (Chung et al., 2017)

Chapter I Research design

1.1 Research question

Since the DNS is a core protocol within TCP/IP stack, its security is a relevant factor for the Internet. The DNS was not designed with security purposes. By adding a digital signature to the DNS, authenticity and integrity of the data can be guaranteed. In combination with other protocols, the safety of e-mail can be increased. Although it is difficult to quantify the risk of missing DNSSEC, for policy makers there is enough reason to design a policy to increase adoption.

The properties of DNS are of a technical nature, but adoption of DNSSEC raises economical and juridical questions. The decision to adopt DNSSEC is based on a rational decision, balancing benefits and drawbacks. Some technical details and pros and cons of DNSSEC are discussed, but the thesis will not explore these questions in detail. The status quo about the value of the DNSSEC solution will be taken as a starting point.

To limit the scope of this research, only the Dutch market is investigated. Since there are several top-level domains[9], only the top-level domain .nl is analysed in this research. Different top levels entail different stakeholders. The Internet Engineering Task Force (IETF) and Internet Corporation for Assigned Names and Numbers (ICANN) set standards for the Internet all over the world, but in this case the focus is on the specific context in which Dutch stakeholders operate.

As research of SIDN has shown, there are quite large differences in adoption levels between sectors. The (semi-) public sector has in 59% a signed domain name, but in other sectors like ISPs this is much lower (22%). This while at the moment on average 49% of all domain names are signed. Since there are considerable differences in signed domain names between sectors, question is what causes these differences. This brings us to the central research question:

How can the variance in adoption levels of DNSSEC signed domains in the sector (semi-) public institutions and ISPs be explained?

More specifically the following questions are answered.

- What actors provide DNSSEC?
- What are explanations for the adoption levels in the (semi-) public sector? What possibilities are there for the policy maker to increase adoption?
- What are explanations for the adoption levels in the sector Internet service providers? What possibilities are there for the policy maker to increase adoption?

In this *first chapter,* the analytical framework and the methodology is discussed (next to this introduction and illumination of the research question). The analytical framework is constructed to create a viewpoint to explain observed adoption levels. In the methodology part the applied research methods are discussed, including the use of interviews. In the *second chapter,* the DNSSEC solution as designed by IETF and ICANN is briefly explained. Also, a stakeholder analysis is conducted, including

[9] There are many top-level domain names (tlds). Well known are .com, .info, .net, and .org domains. Also .biz, .name, en .pro domains can be considered generic. The .nl extension is an example of a Country-Code Top-Level Domains, that is reserved for countries and political entities. In 2013 ICANN decided to admit more top-level domains, sponsored as well as non-sponsored tlds.

incentives on supply and demand side (that vary per sector). This is done by using literature, by data gathered by interviews with representatives of several stakeholders, and comparative research. A representative group of ten individuals are interviewed, representing registry, registrar, registrants, and the (semi-) public sector and ISPs. It is important to note that the same actor can have multiple roles (see appendix II for an overview).

In the *third chapter,* an explanation is provided for the adoption levels of signed domain names within the (semi-) public sector. The same is done for the ISP sector in the *fourth chapter*. This by analysing existing regulation, in combination with data gathered from stakeholders. It includes (expected) legislation, like the Wet generieke digitale infrastructuur, and suggestions for possible refinements.

1.2 Research relevance

With the rise of ICT cybercrime also increased. The total number of cybercrime incidents in 2016 is approximately 2,5 million (CBS, 2017). In the Netherlands in 2015 about 11% of the population became victim of cybercrime (Centraal Planbureau 2016; 6). Out of 100 citizens about 19 were a victim of cybercrime (some people were confronted with more than one incident in a year). The real impact is probably higher, because in a relatively low number of cases the police was informed. Around 8% of the (estimated) total number of cases were notified, this probably due to lack of confidence in espial methods. (Centraal Planbureau 2016; 7)

The most used medium to spread malware is e-mail. E-mail by itself is not protected against eavesdropping, forgery or manipulation. For an average user, it is very hard to establish the authenticity of the sender. Also, phishing mails are getting better and it is becoming difficult to establish the difference between an original message. In 2016 91% of the cyberattacks started with phishing. (NCSC, 26). This makes phishing the most common cause of cybercrime. (Centraal Planbureau 2016; 9)

Mail security is inextricably tied to (the security of) the DNS. A network attacker can spoof the DNS records of a mail server, to redirect mail connections to a malicious server[10]. So, if the DNS is not secured, other protocols that are used on top of the DNS are of less value. Out of the publicly accessible DNS servers around the world, approximately 2% of the global domains provide an invalid IP address or mail record.(Durumeric et al. 2015; 34)

It is difficult to add numbers to cyber security incidents that occur because of the unsecured DNS. The DNS is one protocol in a stack, that all together provide a service. There are not many known cases related to the abuse of the DNS. Another problem in determining costs is the lack of data, including social impact (Ganan, 2017). There are only rough estimations of the costs of cybercrime as a whole in the Netherlands[11]. A report by Deloitte estimates the total costs for the Dutch economy at about €10 billion on a year basis (Deloitte 2017; 6).

In a model by Anderson several elements are distinguished in calculation costs. *Direct losses* are the damage felt by the victim, such as withdrawal from the victims account. *Indirect losses* caused by cybercrime such as loss of trust in online banking or opportunity costs when customers do not trust e-mail to communicate with their bank. Indirect costs occur regardless whether an attack was successful

[10]Taking over business e-mail accounts and spoofing by cyber criminals can have a huge impact. In one occasion a victim transferred $400,000 USD to a bankaccount owned by criminals. (XR Magazine, 2017)

[11] In certain sectors such as payment services there is reliable information available about fraud, see for instance the annual report of the Nederlandse Betaalvereniging (Nederlandse Betaalvereniging, 2016).

or not. Measures to prevent cybercrime such as fraud detection are examples of *defence costs*. The costs to society is the sum of direct losses, indirect losses and defence costs. (Anderson et al. 2013; 5-6)

Unsecure e-mail comes with substantial costs. The *Berichtenbox voor bedrijven* can be regarded as an example of defence costs. Because of unsecure e-mail, the department of Economic Affairs offers a secure alternative for e-mail. With the Berichtenbox entrepreneurs can exchange messages like notifications, permits or subsidy request with the government in a secure way. The department of Economic Affairs spends € 2 million a year on the Berichtenbox voor bedrijven.

The Dutch government and engaged companies started in February 2017 a coalition for a safer e-mail (Internetstandaarden, 2017). Goal is to secure e-mail by preventing eavesdropping and phishing. By adding Internet security standards in the e-mail stack, e-mail can be better protected. Sender policy framework (SPF), Domain keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) are three protocols based on DNS to fight spam, malware, and viruses. (DNSSEC; 2017a)

With DNS-based Authentication of Named Entities (DANE) the DNS protocol is extended with a record, that can provide information about the server certificate. If both sites support DANE, a secure connection can be enforced. This prevents manipulation by an attacker. These standards together should make sure that a sender cannot be forged, a message cannot be changed or read by a third party. (Nationaal Cyber Security Centrum 2016; 26)

There are also several other ways for phishing, without abusing the DNS. This can be done for instance by URL-spoofing. The URL of a bank can be mimicked, so the end-user thinks the real website is visited, while this is actually a fake one. Phishing can be done by using other sign sets in domain names, that actually look like the real URL. Compromised domains can be masked with URL shorteners, so the visitor cannot determine the real web address that is visited. Also, there are only a few known cases related to the abuse of DNS.

In sum this means that the actual damage or relevance of the abuse of the DNS is hard to determine. There are no reliable figures about the damage done by cybercrime related to the DNS. The vast majority of cybercrime starts with e-mail, but there are a lot of other ways to manipulate the end-user other than by abusing the DNS. The actual effect of securing e-mail by using DNSSEC on phishing is therefore hard to establish. It is clear that DNSSEC enhances the security of e-mail, but the exact impact remains unknown. For private parties this is a point of concern, since the decision to invest is based on the expected return-on-investment.

For policy makers that operate within the public domain the question about the relevance of DNSSEC solution is less important. The adoption of Internet security standards enhances the trust of end-users (citizens) in digital (government) services. This trust is a driver for innovation and adoption of digital services. The risk appetite within the government is very limited, each incident is considered one too much. The policy of the department of Economic Affairs is therefore aimed at increasing adoption of DNSSEC. To design such a policy, an in depth understanding of actors and incentives can be helpful. The thesis proceeds from the viewpoint of the policymaker.

1.3 Analytical framework

1.3.1 Market failures

The dominant perspective on cyber security issues is still largely of a technical nature. If we have better security measures available, such as firewalls, reliable identity management, two factor authentication, security issues will be solved. But many security incidents show that despite available solutions, this is not the case. As the work of Ross Anderson in the early years of this century demonstrated, many security problems can be explained better by using microeconomic theories (Anderson, 2001; 1). In other words, 'technology changes, economic laws do not' (Katz & Shapiro, 1985; 1)

These theories explain convincingly the occurrence of threats we are confronted with, such as phishing, data leakage, ransomware and so on. End-users often carry the burden of (lack of) security decisions made by other participants in the network. Security failure is caused not only by bad design, but at least as much by misaligned incentives. (R. A. T. Moore 2006; 1) Due first mover advantages, it is usually not attractive to invest in security measures.

In ideal circumstances – perfect competition, no public goods – markets are efficient and can create a Pareto optimal situation. No one can gain, without at least one person losing something (Arrow and Debreu, 2007, 265). But there are several forms of possible economic problems adhered to cyber security measures. In economic terms, the suboptimal level of implementation can be understood as 'market failure'. A market failure exists if the allocation of goods or services are not optimal distributed. If this is the case, the pursuit of self-interest by actors do not lead to an efficient outcome. From a societal point of view there is room for improvement.

Although there are technical issues that come along with the implementation of DNSSEC, these issues are not the only cause of the limited adoption. This thesis focusses on the economic reasons for this limited implementation. Goal is to see if concepts retrieved from microeconomics like externalities, asymmetric information, liability dumping, and the tragedy of the commons can explain the observed implementation levels of DNSSEC. In this perspective key question is whether costs and benefits for market players are aligned with social costs and benefits.

In the theoretical framework, the applicable failures for DNSSEC are identified. This is done by analysing stakeholders and accompanying incentive structure. Who will gain from implementing DNSSEC and who will pay the costs? The premises are validated during interviews with stakeholders. This will explain a main question: given the costs of cyber security attacks, why is there not more investment in security measures? (Friedman 2011; 9).

Market failures occur when decisions of companies and consumers do not lead to an optimal socially desired level of security. Microeconomic theory in general distinguishes five forms of market failure. 1.) A transaction can have effects for third parties (externalities). 2.) An operator on the market knows more about the product than a consumer (information asymmetry)[12] 3.) Reduction of solutions offered to market to make more profit (monopoly). 4.) Not acting according incentives or irrationality 5.) Uncertain aspects in the future make it difficult to agree on contracts (incomplete contracts). (Centraal Planbureau 2016, 4) (Anderson 2001; 1-7)(R. A. T. Moore 2006; 1-9).

[12] The .nl extension is usually seen as more trustworthy than other domains, such as .org or .biz.

These market failures cause problem areas within the Internet domain. In the case of the DNS, this results in vulnerable applications and infra-structure. This because applications are built on top of the DNS. As a result, end-users are exposed to threats like phishing, ransomware and data-leakage.

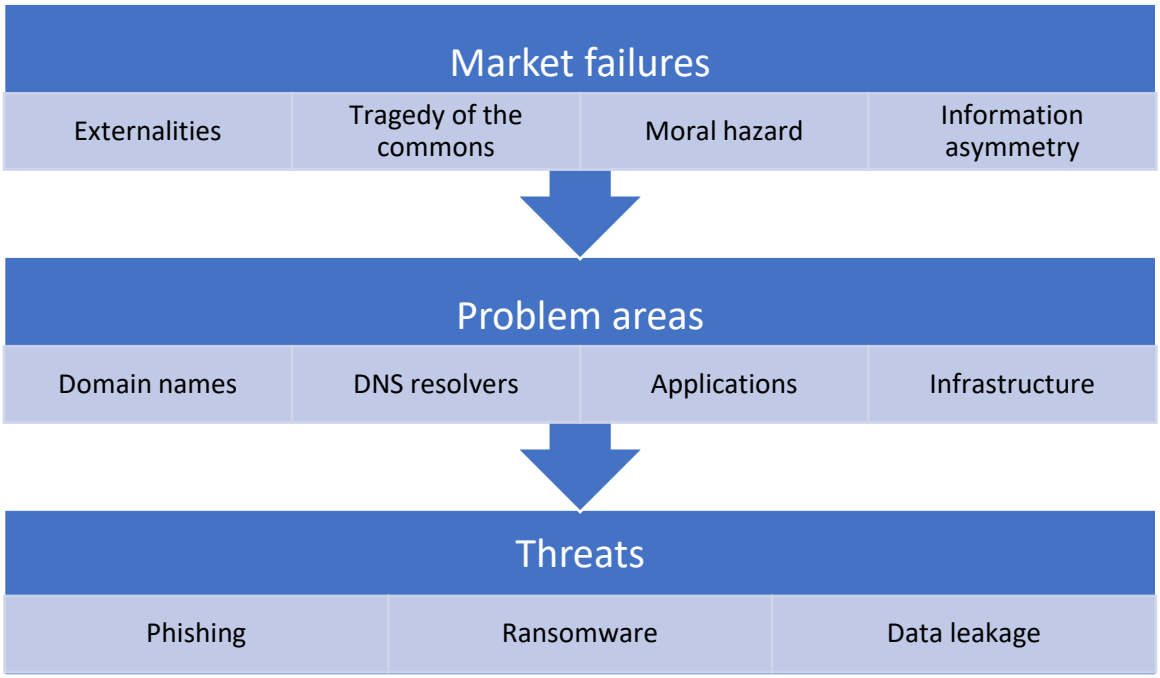


Figure 1 Analytical framework, partly retrieved from Centraal Planbureau (Centraal Planbureau 2016, 5)

In the economic perspective actors decide on the implementation of cyber security measures based on incentives. These actors often do not carry the (full) burden of lack of security investment. In the case of DNSSEC, ISPs that offer hosting and access services must invest to provide DNSSEC. But the ISPs do not suffer the consequences from for instance insecure e-mail. The cost of a suboptimal level of investment in cyber security measures are borne by the end-user. The end-user user has to mitigate the risk level on the customer side. This is a market failure generally referred to as an externality.(Moore 2010; 3) This means that the social costs are more than the private costs (the difference is the negative externality).

Another important aspect in the functioning of a market is trust. Trust can be distorted by information asymmetry. As Akerlof in his essay The Market for lemons noted 'Distinguishing good quality from bad (..) may in fact be one of the more important aspects of uncertainty' (Akerlof 1970; 500). Information asymmetry exists when a seller knows more about a product than the buyer. In this case, it is hard for a buyer to establish the quality of a certain product.

The end-user can check if a secure connection is used for a website by a lock in the browser. For DNSSEC, it is much more difficult to tell. Only with the use of tools like Internet.nl or with a browser extension (as there is for example for Firefox) it becomes clear that DNSSEC is used. Also, if it is clear that DNSSEC is used, the advantages are not obvious. Most registrants are oblivious of the advantages for them. Of course, suppliers of hosting services and access services are aware of these advantages,

but ISPs do not profit from implementing it. (Friedman 2011, 11) In most cases the user just presumes that the .nl extension in general is reliable (more than .org, .info etc).[13]

ISPs will only add services like DNSSEC, if there is an incentive to do so. This incentive consists of a higher price for a domain name, hosting or access service. But if there is no demand because a registrant or end-user is not aware of DNSSEC, there is little incentive to do this. So, it is not very surprising that only around 10% of the registrars offer DNSSEC. This can be considered a 'chicken-and-egg' problem.(Ozment and Schechter 2006; 12).[14]

Suboptimal investment in cyber security measures lead to social costs. The consequences of the lack of security measures are borne by the end-user, not by ISPs. Rational choice theory assumes that only costs borne by the actor itself is considered. Social costs consist of private investments and externalities. In the case of a negative externality social costs out weight private costs. Social costs (and market failures) can be considered a ground for government intervention.

1.3.2 Regulation

According to the policymaker the pace of DNSSEC adoption (and other Internet security standards) is too slow. Government intervention can be shaped in many ways. There is a classical model based on 'command and control'. This could entail proscribing a standard as an obligation. Another option is self-regulation. The industry can put forward its own strategy to implement a security standard. Finally, this also could be done by co-regulation (Lodge and Wegrich 2012; 96)

Government intervention in markets is a much-debated question. Regulation can play an important role in addressing market failures, but it has drawbacks. One of the arguments against regulation is that it interferes with efficiency of the market. It distorts market efficiency and the benefits of regulation are only profitable for certain groups. But regulation, if well designed, can also ensure that markets provide more equitable outcomes (Stiglitz 2008; 25) But how to design a policy? At the moment, there is not much legislation in the Netherlands about Internet security. [15]

To examine what such a policy should look like public interest theories will be used. Key concept in this theory is that regulation can help to pursue collective goals. In this case DNSSEC is perceived as a part of the cyber security level the end-user experiences. The market for DNSSEC is examined to determine to what extent market failures can be identified. Market failures result in risks, that are inflicted upon the end-users. According to public interest theories economic regulation can help to 'fix' market failures (Stiglitz, 2008; 3). Correction of failures can increase general welfare, that serves the public interest. In this case, the exposure of end-user's sensitive data like financial or personal information, because of a lack of incentives to implement DNSSEC.

[13] This is usually correct. The adoption of Internet security standards for the .nl domain is much higher than the worldwide deployment.

[14] The basic concern of the end-user is to how to choose a suitable domain name that is still available.

[15] Except for the Telecomwet. In this law, there is a provision (art 11.3, 2e provision) that ISPs have to provide a secure network (beveilingsplicht). The Autoriteit Consument en Markt enforces the Telecom law, but in practise it is very difficult to use against ISPs. ("wetten.nl - Regeling - Beleidsregels informatieplicht voor aanbieders over internetveiligheid (artikel 11.3 tweede lid van de Telecommunicatiewet) - BWBR0033401," 2013)

There are two characteristics of a public good, that distinguishes it from traditional goods. In the case of a public good, enjoying the advantages will not prevent someone else from doing so (non-rivalrous). It is also not possible to exclude someone from enjoying the advantages (non-excludable). These characteristics make it impossible for a private company to establish a price. Well known examples of public goods are (expenses for) infrastructure to prevent water flooding. This is a classical task for the government. So cyber security has strong characteristics of a public good (non-rivalrous and non-excludable), the increase of standards as DNSSEC can be considered of public interest. (Moore 2017; 1)

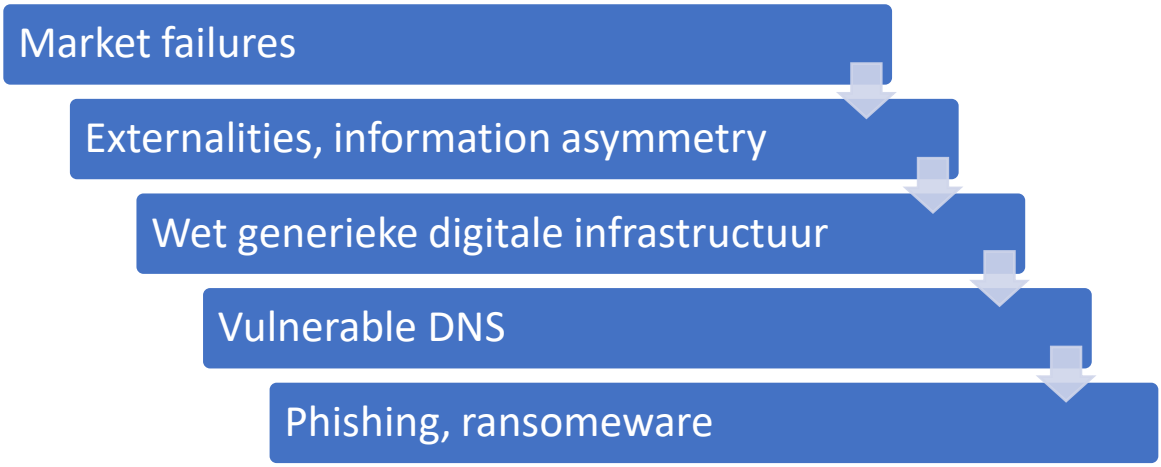


Figure 2 Market failure is a legitimation for government intervention

A way of analysing regulation is to study the division of responsibilities between the government and private actors. Government intervention basically oscillates between setting and enforcing a security baseline on the one hand, and just use government's buying power to encourage best market practices on the other hand. The characteristics of the field determine the best approach. (Friedman 2011; 11)

These characteristics are studied in two sectors (semi-) public institutions and Internet service providers) that have been chosen to explore reasons for (not) adopting the DNSSEC solution. By analysing the incentives, the different stakeholders have, feedback loops can be determined. Also, the incentive structure is of interest for the regulator, to determine what kind of feedback loops exist.

According to Laurence Lessig there are four domains ('constraints') that regulate behaviour. (Lessig 2006, 122) One constraint is legal. The law determines what you can and cannot do. Laws can be used to include externalities. In the US, the banks have to prove that the customer is mistaken or lying in the case of a fraudulent transaction. In the Netherlands, it is the customer that has to prove that the bank was mistaken. As a result, US banks suffer much less fraud. In this way the law can internalise the effects of externalities. (Anderson 2001; 1)

Another constraint is the market. Markets determine the price of a domain name, that put a constraint on the number of domains you can obtain. If the price is changed, then this will affect the behaviour of the registrant. This also goes for quality. If the market provides a huge variation in domain names in

price and quality, the choice of domain names also increases. Increasing choices means reducing the constraint.[16](Lessig 2006; 123)

1.3.3 Policy options: the (semi-) public sector

According to Friedman, characteristics of a sector determine the best approach for the regulator. Within the (semi-) public sector, the regulator has relatively many options to stimulate adoption. There is a direct relation between a (semi-) public institution, and a signed domain name. By addressing responsibilities to (semi-) public institutions to use signed domain names, the adoption of DNSSEC can be advanced. Responsible employees within the (semi-) public sector can request a signed domain name, as supplied by their vendors. This as far as the signing side is involved, validation on the access side is mainly provided by private companies to end-users.

Basically, the current strategy is based on the comply-or-explain policy as designed by the Forum Standaardisatie. Organizations within the (semi-) public sector are supposed to implement Internet security standards, unless there are legitimate reasons not to do so. This can be done by requirements a supplier has to meet. Services delivered by private software vendors must adhere to security standards used by the government. (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2017; 2) This can be considered setting a good example by the (semi-) public sector.

The Wet GDI that currently is being prepared is about taking the comply-or-explain policy one step further by setting a standard. To increase the adoption pace, the law introduces an obligation for (semi-) public authorities to use Internet security standards (like DNSSEC, but also other protocols like DKIM, etc.). This is done by an *Algemene maatregel van bestuur* (Ministerie van Economische Zaken 2017, 6). This will be done 'if necessary and proportional' and if needed for 'good working, safety, reliability, and efficiency of electronic traffic'. (Ministerie van Binnenlandse Zaken 2017; 1)

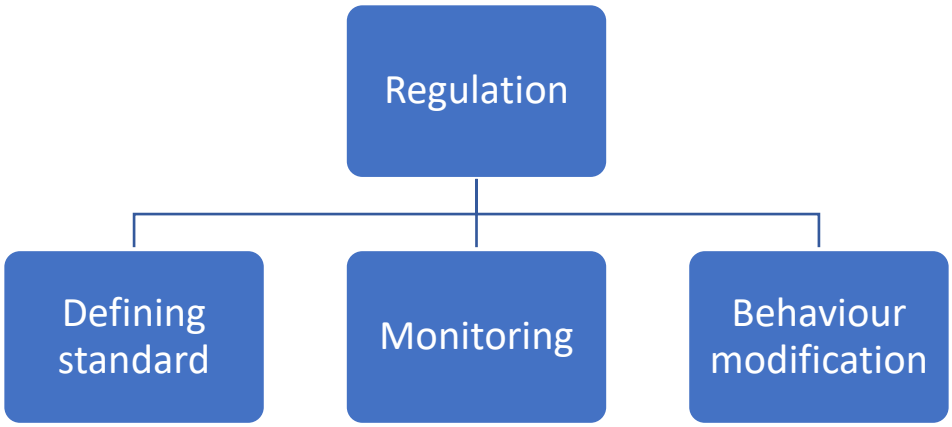


Figure 3 Regulation as setting a standard (Black 2002, 26)

Setting and enforcing a security standard is a rather intrusive measure. Part of the research entails the effectiveness of this law. Just what exactly is 'when necessary and proportional', and needed for 'good working etc'. To do this the principles for effective regulation (Lodge and Wegrich 2012; 54) are used.

[16] Lessig also distinguishes social norms and architecture as constraints, but these are not discussed here. Technical details of the DNS can be considered architecture, in the way that they determine functionalities (and the implementation process).

These are the following principles.

1. Proportionate
2. Accountable
3. Consistency
4. Transparency
5. Targeted

To apply these principles additional documentation is analysed, such as definition and scope. Just exactly what does a (semi-) public institution have to do to implement DNSSEC? What actors are included? Are the required measures proportionate? What infrastructure is in or out of scope? This to determine whether this law is well designed, and if there are other options available to ensure profitable outcomes.

1.3.4 Policy options: the ISP sector

The ISP branch is quite different from the (semi-) public sector. Most companies are privately owned, and range from small to large businesses. The ISP sector is a very innovative and highly dynamic market, and regulation is designed not to interfere with this. One of the challenges for policy makers is how to increase the adoption of Internet security standards in a predominantly privately-owned infrastructure. This entails signed domain names within this sector (including hosting), as well as DNSSEC validation by access providers. There are several options to do this, ranging from intrusive to cooperative approaches[17].

- *Introduce or adjust regulation*

On the one side of the spectrum of possible interventions by the policy makers is regulation. An option is to adopt established security standards as an obligation, like is being prepared in the Wet GDI (the ISP sector is currently out of scope in this law). This entails focussing on security practices, often based on formal specifications. Setting and enforcing a standard is a form of *ex ante* regulation (T. Moore, 2010; 8). It generally includes standard setting (rule itself), behaviour modification, and information gathering (Lodge and Wegrich, 2012; 13-14)

Compliance is designed to enforce a minimum standard of security. Standards should contribute to a reduction of a security incident. Ideally, this reduction should be in line with the appropriate risk reduction.(Friedman, 2011; 12) Setting and enforcing a standard or baseline is an intrusive option. Regulation can have all kinds of (international) side and ripple effects. Another problem of intervention is enforcement. How to make sure that rules and incorporated? Opponents of this kind of regulation also point out the increase of the regulatory burden.

Next to compliance an approach could be based on sanctions, *ex post* regulation. This can be done for instance by creating transparency and a responsible disclosure policy. Damage for companies comes from harming the businesses' reputation or costs for notification. A stronger kind of deterrence can be created by addressing liability. If a company is neglecting a cyber security incident, it can be punished. By the introduction of fines companies can be forced to internalise costs of an attack. Liability could

[17] In a paper by Friedlander three options are listed, 1.) supporting education and public awareness 2.) providing a market for infrastructure 3.) government as lead-by example. (Friedlander, Mankin, & Maughan, 2005)

also include help of the affected individuals. The effects of liability strongly depend on the characteristics of the market. (Friedman, 2011; 13)

- *Increase public awareness*

There are also less intrusive ways market failures can be corrected by the policy maker, ranging from the stimulation of cooperation within the sector to correction of information asymmetry. There is a platform available to enhance the interactions between ISPs, that can be used to shape policy options. This can be done to evaluate existing instruments to increase knowledge of end-users, and discusses other available options.

There are already several tools available for the end-user aimed at increasing visibility of DNSSEC. Internet.nl provides an extensive overview of the security standards that are used for a domain (or e-mail address and connection)[18]. There are also private initiatives, like browser plugins that have a similar function (like Microsoft Explorer, Google Chrome, Mozilla Firefox). Since there are already a lot of icons (for instance https, that is visible in a green lock in the browser), an option is to create or use existing approval mark.

Since these instruments increase the knowledge on end-user side, these instruments (and others) can help to correct information asymmetry. In this way feedback loops can be created. To examine the effectives of these measures feedback loops in DNS eco-system are analysed. Interviews with representatives of the sector help to understand this question and also provide additional information for designing a public policy on this matter.

- *Introduce or extend financial incentives*

Another option is a financial oriented stimulus. In a mild form there already exist an incentive, created by the comply-or-explain policy. Due to this policy, (semi-) public institutions are expected to adopt Internet security standards as DNSSEC. Because of this, companies in the ISP sector that opt for acquiring assignments from these institutions are hold to comply to these standards. It can be expected that this policy has a positive effect on the offering of DNSSEC solutions. The Wet GDI will increase this incentive. This can be considered a 'lead-by' example by (semi-) public institutions.

There are also other financial oriented options for policy makers. Activities that contribute to economical sustainability and otherwise would not have been conducted, can be eligible for a financial contribution by the government. Art 2 of the *Kaderwet subsidies* offers a possibility for subsidies that fit within the Cabinet's policy for the telecom sector(Overheid.nl, 2016b). There is a huge variety of instruments that can shape this policy. Available instruments are for instance subordinated credit, (financial) guarantees, investment incentives or tax cuts. These instruments can be targeted towards the intented policy goal, depending on the characteristics of the engaged sector. For instance, in combination with 'best practices'.

[18] See for this https://internet.nl/

Finally, a public debate about how much security is needed in the ISP sector is very difficult. Public policy makers are controlled by the Parliament, that tends to be over inclusive (Lodge and Wegrich 2012, 43). It will lead to exclude risks, regardless of necessary investments. But complete security is not desirable and not achievable. A very high level of security perhaps also not, which will come at huge costs. From an economic point of view, it is rational to accept some degree of insecurity.

1.4 Methodology

A basic question about methodology is the choice between a quantitative or a qualitative approach. In general, a quantitative approach is more objective and is usually done based on surveys. Drawback of this method is that questions must be formulated beforehand. There is no room for explorative questions. Qualitative research is more suited to answer a 'why' or 'how' question, as is the case in this research. It is possible to add questions during the interview, for instance if the interviewee brings up a new aspect regarding the subject. This in addition to in advance prepared questions. Qualitative research can comprise literature review, case studies, interviews and qualitative analysis.

The research has been done by using case studies. Case studies can provide better insights in detailed behaviour. Essentially there are three types of case studies: exploratory, descriptive and explanatory (Zainal 2007, 2). In an exploratory study the theoretical framework is used as a starting point, that is detailed by examining a certain case (Swanborn 1996; 63). For this reason, the research is designed as an *exploratory case study.*

This can be considered a 'bootstrap' approach (Ozment & Schechter, 2006). Advantage of this approach is, that data can be examined at a detailed level. This is needed to gain more insight in actors and behaviour. There are several stakeholders engaged in providing the DNSSEC solution, and in depth understanding of each position is needed to explain observed adoption levels. A technical solution is available, but incentives for each stakeholder will largely determine if this solution is adopted or not. Another advantage of this approach is, that there is room for unexpected findings (serendipity). Since economic research of cyber security topics is a relatively new field, this is also helpful.

This argument is supported by researchers in this field. Starting point of the research is the assignment for policy makers to increase adoption levels. Policies cannot be shaped based on theoretical models alone. Strategies on public policy are highly sensitive for the specific context. Regulation thus requires an in depth empirical understanding of existing actors and incentives. Therefore, Van Eeten proposes to complement existing economic theories with qualitative field research. (Michel J. van Eeten 2008; 13).

There are also disadvantages connected to case studies. In many cases, it is difficult to generalise conclusions[19]. This because there are many variables that influence adoption. As will be shown, the (regulatory) context has a large influence on this. A prerequisite for generalisation is, that at least a number of the same variables must be available. (Swanborn 1996; 70) Generalisation is also difficult because of the limited number (ten) of interviews that have been conducted.

Qualitative research in general, can lack rigor. To strengthen the approach different research methods are used (triangulation) (Berg 2009; 5). A literature review is used to create a theoretical framework, to which the case studies are linked. For the case studies (semi) structured interviews and comparative

[19] Generally referred to as *pars pro toto* (Swanborn 1996, 32).

analysis are used. There is statistical information available about adopting, in the Netherlands as well as worldwide. This information is used to corroborate presumed assumptions from the theoretical part. The interviews are also used to validate (expected) outcomes of government regulation.

Part of the required data is collected by conducting semi-structured interviews (see appendix I for detailed questions). This means that interviews are conducted based on prepared questions, but there is room to deviate from the questions if an interviewee introduces a new and relevant fact or opinion. The subject of the research is explained to the interviewees, but only limited information was handed over before the interviews.[20]

The research is done by conducting conversational interviews. In conversational interviews, the researcher uses a script of questions, but participants can deviate from questions if relevant. In total ten interviews have been conducted. These consist of three interviews with employees within the ISP sector, three interviews with employees within the (semi-) public sector, and three interviews with policymakers. In addition to this, an employee of a SME company has been interviewed in the role of registrant, and two experts about the added value of DNSSEC.[21] (See appendix II for an overview).

Internet services including DNS are provided by a complex ecosystem of stakeholders. First, the registry (SIDN) plays a role as a trust anchor and zone operator. Most important task of the SIDN is to maintain the toplevel .nl (ccTLD). To do this the SIDN maintains a relation with Dutch registrars, that are obliged to register domain names at the SIDN. SIDN plays a role in advising registrars and other stakeholders about improving Internet security. Two employees of the SIDN have been interviewed about the SIDN policy on providing DNSSEC.

Next, two ISPs have been interviewed. ISPs act as registrars and hosting providers. A different kind is the access provider, that validates DNSSEC answers for their end-user. In some cases, ISPs combine both roles. Two ISPs have been selected that provide both hosting and access services. This on a limited scale, to provide supporting services needed for new platforms ordered by their customers. During the interviews incentives for adopting DNSSEC on the hosting as well as on the access side have been assessed (with a clear distinction between these roles). This to gain detailed insight about costs (investments, education), and benefits (revenues).

The above mentioned stakeholders provide DNSSEC for their customers, and advocate to do so. For a balanced picture, stakeholders that have not adopted DNSSEC should be taken into account. Large access providers like KPN and Ziggo do not support DNSSEC. Unfortunately, KPN as well as Ziggo did not want to cooperate with the research. Since the main findings about investments (hosting as well as access) for ISPs in this research are based on interviews with providers that have adopted DNSSSEC, it is possible that these numbers deviate if the research is conducted on a larger scale, and include other stakeholders.

Central question in this study is what causes the differences in adoption levels of signed web domains in the ISP and the (semi-) public sector. To answer this question interviews have been conducted with representatives of both sectors as *registrant*. It is important to note that the same stakeholder can represent different roles (see appendix II for an overview). The afore mentioned ISPs have also been

[20] In one case (BIT interview) some questions were handed over to establish whether they could be answered by the interviewee.
[21] The total number of interviews exceeds ten because the same interviewee can have multiple roles.

interviewed about adopting DNSSEC for their own domain names. To investigate the incentives for a small- and medium sized (SME) company as a registrant, an interview has been conducted with a medium sized book company. For the (semi-) public sector the Dienst Publiek en Communicatie, DICTU and Logius have been interviewed. This to gain insight on motives to adopt DNSSEC in the (semi-) public sector.

The above mentioned registrants operate within a regulatory regime. The different regimes for both sectors have been taken into account to investigate to what extent the prevailing regimes influence the adoption of DNSSEC. To do this interviews have been conducted with the policy makers in both sectors. The department of Economic Affairs is responsible for the Telecomwet, that sets conditions within this sector. Forum Standaardisatie plays an important role in encouraging the adoption of Internet security standards like DNSSEC within the (semi-) public domain name. Both policymakers are also engaged in the design of the Wet GDI. The Dienst Publiek en Communicatie (DPC, part of the department of General Affairs) has been interviewed about implementing a policy for the (semi-) public sector to increase the adoption of Internet security standards (like DNSSEC).

Finally, two interviews have been conducted about the value of DNSSEC from a technical perspective. This to validate conclusions retrieved from literature study. These interviews have been conducted with two members of the expert committee of the Forum Standaardisatie.[22]. As shown in this thesis the (technical) benefits of DNSSEC have to be balanced with expected return-on-investment for engaged stakeholders.

As noted, only a limited number of ten interviews have been conducted. These interviews had to be dispersed between several stakeholders engaged in the DNS ecosystem, that are quite numerous. In addition to remarks about limitations of qualitative research, the limited number of interviews imply that conclusions of the research have a tentative character. This goes for instance for the presented investment figures, as discussed above.

1.5 Reflections

This research design also has drawbacks. Our analytical framework is retrieved from classical economics, so criticism about this approach is also applicable on this thesis. In classical economics, the 'homo economicus' is a central paradigm. People are rational, make decisions based on incentives and self-interest. Behaviour of people can be analysed by studying incentives and interest. Based on this, behaviour of people and other actors like companies can be explained.

At the end of the 20th century behavioural economists like Herbert Simon showed that people are only to a limited extent rational. In many cases, all kind of imperfections – like emotions, incomplete information, environment – influence outcomes of decision making. Since our rational capacities are limited, there is 'bounded rationality'. So behavioural economics show (human) actors in certain circumstances as far from rational (Simon 1952; 99-100).

For explaining regulation public interest theories are used. These theories comprise that legislators responsible for design and implementation of legislation aim at collective goals of general welfare of the community. This can entail economic regulation, but also broader political goals. Contrary to public interest are private interest theories, that hold individuals or groups accountable for legislation to

[22] Interview with J. Guillen Scholten PhD, architect DigiD Logius and Roland van Rijswijk-Dei PhD, manager SURFnet and assistant professor at University Twente.

increase their self-interest. In this libertarian view regulation may promote public interest, but if this is the case it is a coincidence. Government intervention is also prone to government failure.(Stiglitz, 2008)

The analytical framework is constructed to analyse the adoption of an Internet security standard. But a model always is a reduction of complexity, where aspects need to be left out to study certain phenomena in more detail. The framework is designed to get a better understanding of complex processes that can be observed. Of course, other angles can be used to increase the understanding of implementing security standards.

Also, some remarks can be made when it comes to calculation costs of cybercrime. Cyber security is actually a non-event. Like intelligence, it is a 'latent construct', it cannot be measured directly. Cyber security can only be known through it properties. Controls are added to mitigate risk. These controls are supposed to increase security, but many times this is unknown.(Asghari, van Eeten, & Bauer, 2016). The absence of incidents is no evidence that controls are effective. Actually, it is very hard to measure the effectiveness of controls like standards, certification and auditing. This makes it very difficult to calculate the return on investment, needed for the business case to persuade decisionmakers.

Although the topic of this thesis is technical in nature, the attribution of this thesis is not in the technical field. The current status quo of the technical community about DNSSEC solution is taken as a starting point. The main contribution of the thesis is a more detailed analysis of stakeholders and incentive structure for implementing DNSSEC. There are already several studies available that analyse DNSSEC implementation from an economic perspective (T. Moore, 2010)(Friedman, 2011)(R. A. T. Moore, 2006). But these are more general studies, that do not take specific legislation or sectors into account. Since regulation (in this case Dutch) has a significant impact, these factors are considered in this study. It will shed light on factors that impede (and accelerate) the implementation of Internet security standards in different sectors in the Netherlands.

Chapter 2 Actors and the adoption of DNSSEC

The DNS is a core protocol within the TCP/IP stack, but it is not designed with security in mind. In this chapter at first essentials of a DNS secure solution are described, including creating a chain of trust. Next several roles of actors that supply the DNSSEC solution are analysed. It is important to note that the same actor can fulfil multiple roles.

2.1 Working of DNSSEC

The Domain Name System is based on hierarchical domain names. This system allows levels to be added to the top-level domains, such as .com, .nl, and .edu). A second level microsoft.com can be added, a third info.microsoft.com and so on. Each domain name has to maintain a database ('zone file'), containing IP addresses associated with all the sub domains lower in the hierarchy. So the operator of the .nl domain has to maintain a server with all the IP addresses for the 2e level in the .nl domain and so on. (Post and Kehl 2014; 4)

The vulnerability of the DNS remained a theoretical question[23], until Dan Kaminski proved in 2008 that DNS flaws could be used in 'cache poisoning' (Pham, 2016)[24]. This attack uses the limited number of transaction IDs within DNS-messages. These numbers are used to link DNS questions and answers from the client and the nameservers. If a false answer can be sent using the right transaction ID by the resolver, a false IP- address can be injected in the cache of the client. (DNSSEC.nl, 2017) These attacks are not very common, but this can change if vulnerabilities are discovered that make easier type of attacks possible[25]. (ICANN, 2017)

The Domain Name System Security Extensions (DNSSEC) is a set of extensions of the DNS, that provide DNS clients (resolvers) authenticated DNS data. The main functions of DNSSEC are authentication and integrity of the data (Rijswijk 2017, v). Clients that validate DNSSEC, receive address information, including a digital signature. By checking this signature, a DNS client can determine whether the provided information is the same as published by the zone owner. It also includes authenticated denial of existence. (Antić 2014, 678). DNSSEC is backwards compatible, hosting and validating ISPs can cooperate with systems that have not applied DNSSEC. (DNSSEC.nl, 2017)

Most relevant is the risk of unsafe DNS by using e-mail. This because the e-mail protocol (Simple Mail Transfer Protocol SMPT) has default no security measures. Standards are designed to make Transport Layer Security (TLS) and DNSSEC work together. STARTTLS makes it possible to guide e-mail (SMPT) by using a secure TLS connection. Based on the statement of an interviewee, the lack of security of e-mail urged the Dutch Tax department to physically visit companies to exchange certificate keys (Interview SURFnet). STARTTLS in combination with DNSSEC solves this problem.

In the case of e-mail, there are always two servers involved. To establish the authenticity of a server mostly self-signed certificates are used. So, there is always a risk to communicate with a malignant server. By using STARTTLS the connection between mail servers is encrypted. If the sending mail server

[23] For an overview of specific threats see an article by The Internet Society, 'Threat analysis of the DNS' (RFC 3833). (Atkins & Austein, 2004)

[24] See for example how this works http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

[25] This does not have to be the case. Many cyber security incidents that could occur did not materialize (Zittrain, 2014; 9).

supports DNSSEC, then the receiving server can validate the signed domain name. When both sites use DNS-based Authentication of Named Entities (DANE), it is possible to enforce the use of STARTTLS. In this way it is possible to secure e-mail against eavesdropping. (Internetstandaarden, 2017)

To make sure e-mails are send from an authenticated domain, Domain Keys Identified Mail (DKIM), Sender policy Framework (SPF) and Domain-based Message Authentication Reporting and Conformance (DMARC) can be used. This by protecting the sender (e-mail address, mail system) and the content of an e-mail message. To do this a new record is admitted to the DNS-information. Although DNSSEC is not necessary to use these protocols, for instance for DKIM it is an addition.[26]

A first version of the Domain Name Security Extensions (DNSSEC) was accepted by the Internet Engineering Task Force (IETF) in 1999 (IETF, 1999) and reviewed in 2005 (RFC 4033, 4034, 4035) (IETF, 2005). These documents describe in detail the characteristics of the added record types and modifications of the DNS records. In 2014, the Internet Corporation for Assigned Names and numbers (ICANN) made DNSSEC an obligation for all new generic TLDs. (DNSSEC, 2017a).

This is important because a prerequisite for the chain of trust is a signed top-level domain. There are several registries that are responsible for top level domains (TLD), and for issuing domain names to registrars. The authenticity of the records can be checked with a public key, connected to a specific domain name. This key is published by the registrar. The client can check if the public key provided by the name server is the same as the one that is listed by the registry. In this way, a chain of trust is built over the several levels of the DNS-hierarchy. [27]

[26] For this reason, the Department of General Affairs, that registers central domain names for the government, shuts down default e-mail functionalities when a domain is issued. This to prevent fraud. Only if all protocols to secure e-mail are supported, mail can be used for this domain (Bestuur, 2017) .

[27] There is also certificate pinning that protects an end-user against fraudulent websites. This does not cover the complete DNSSEC solution. For instance, it is possible to register a website that looks very much like the one of a bank, for example i-ng.eu. A hacker can request a certificate for this website by a Certificate Authority (CA). As a next step, the DNS of ING can be adjusted to i-ng.eu and the end user gets the green mark at the lock because the certificate is validated by the CA.

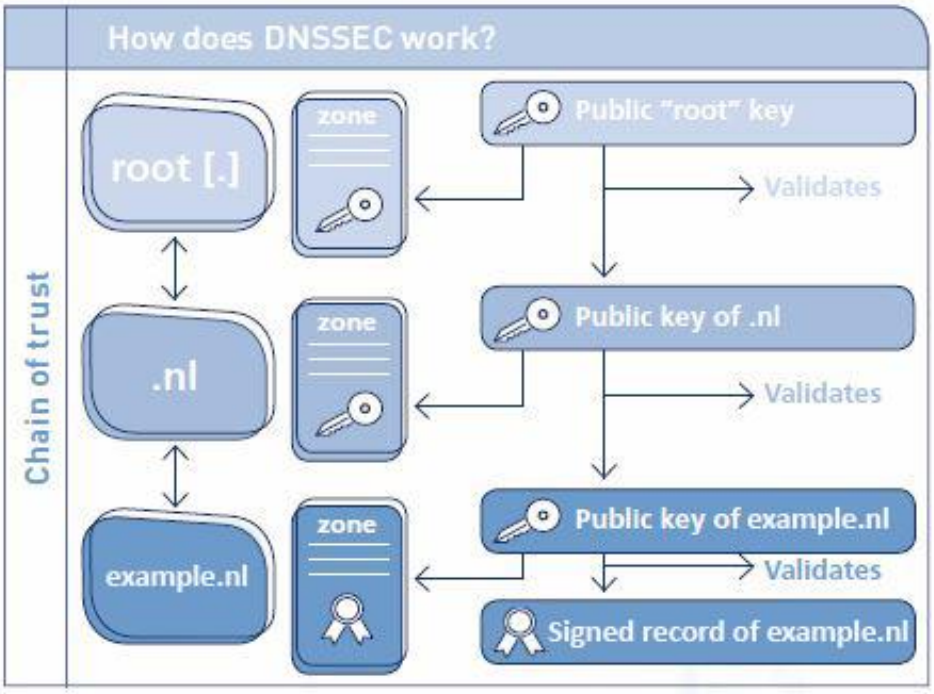


Figure 4 The chain of trust for a signed domain (SIDN, 2017b)

The SIDN is responsible for maintaining the top-level .nl domain name and accompanying infrastructure. For a .nl domain name, the public key is available on the name servers of SIDN that control the .nl top level domain. This makes it possible for registrars to issue domain names with cryptographic signature for registrants. Registrars act as man-in-the middle between registries and registrants. They provide domain names, including the (optional) support of DNSSEC. (SIDN, 2017c)

DNSSEC signing is only valuable when the signed domain names are checked by validators (of the end-user). To make sure that the translation of a domain name to an IP address is correct, the whole chain must be secured. This not only goes for the chain of trust and all engaged DNS servers, as just described. The caching DNS servers of an Internet access provider and the client of the end-user also have to support DNSSEC. Most clients used by the end-user consist of a simple resolver handling all DNS lookups. The actual validation (recursive queries) is left to the caching DNS servers. This typically occurs on the infrastructure of an Internet access provider. (DNSSEC.nl, 2017)

A vast majority of the Internet access providers do not support DNSSEC. KPN and Ziggo (market share 80 - 85%) both have not adopted DNSSEC. There are a few Internet providers that do validate DNSSEC for their end-users. These are usually smaller companies like XS4all, BIT, and Edutel (Stichting Internet Domeinnamen 2017; 5). These companies all together have a limited market share. For controllers of smaller networks, there are tools available to support DNSSEC. (DNSSEC.nl, 2017)

No holy grail

Since the introduction of DNSSEC several technical experts pointed out disadvantages connected to DNSSEC[28]. Because of the longer messages, domains that use DNSSEC can be less well accessible. If a message is not correctly signed, this can lead to unreachable websites. It means that an end-user with a DNSSEC validating provider gets an error message while visiting a website, and another end-user that uses a non-DNSSEC validator can access the website without a problem. For ISPs that are a gateway to the Internet for their customers, this is a critical issue.

This problem is closely monitored and due to addressing registrars in the case of a bogus domain names the problem has diminished, according to the SIDN (Interview SIDN). The number of bogus domain names declined from 4% at the start to the current level of 0,0012% (DNSSEC, 2017b). ISPs as BIT, that also provide access services for their customers, have confirmed that these problems have largely been solved. The number of phone calls to the helpdesk of BIT have declined from three a day to about one per month (Interview BIT).

Another drawback is a vulnerability for DDoS attacks. Because of the added signature DNSSEC responses are longer than DNS responses. This extra size makes DNSSEC more vulnerable for DDoS attacks. By using flaws in DNSSEC, it is possible to amplify the number of sent packages many times. This is generally referred to as 'amplification attacks'. By using this vulnerability, it is possible to take down a server. Amplification attacks were used for very severe DDoS attacks. The use of DNSSEC can accelerate amplification on average about 6 to 12 times[29]. (Rijswijk 2017; viii)

Also, DNSSEC protects the name server and the transport of DNS-information to the client. The client itself is not protected. If a PC is infected with malware, usually the resolver (part of the operating system that translates domain names into IP-addresses) and the local cache can be manipulated. In many cases, the end-user is not aware of his computer being infected with malware. (DNSSEC, 2017a)

2.2 The registry

In many cases the initiative for deploying DNSSEC comes from a registry that operates a zone. There is an incentive for registries to provide a secure solution for registrars. Maintaining the .nl top level (ccTLD) is a task of the SIDN. The SIDN functions as a trust anchor, a prerequisite to offer DNSSEC. Often registries have a role as a lead-by-example to provide secure solutions for their domain. Also, the registry for the top level domain offers ISPs help while facing problems deploying DNSSEC, so deployment becomes less difficult. (Enisa 2012, 41) Since 2014 there is an obligation for TLDs registries to provide DNSSEC.[30]

[28] These disadvantages have made several authors oppose the DNSSEC solution. For instance Cowperthwaite has argued that DNSSEC compromises availability of websites, that has brought him to the conclusion that 'the cost-benefit analysis clearly shows that DNSSEC deployment is a futile effort, one that provides little long-term benefit yet has distinct, perhaps very significant costs'.(Cowperthwaite & Somayaji, 2010). In an article by Kieren McCarthy named 'Is DNSSEC causing more problems than it solves?' the increased risk of a DDoS attack is illuminated.(McCarthy, 2016)

[29] This caused by the default choice for RSA as a signature scheme for DNSSEC. The keys and signatures continue to grow due to raising security requirements. There are alternative signature schemes available like Elliptic Curve Cryptography, that generate much smaller keys.

[30]. Ibid.

It took engineers of the SIDN several weeks to switch on validation on the resolvers of SIDN. There were no investments involved, costs consist of working hours from employees. The signing of the TLD is more complex. A complete 'signing street' had to be developed, including several hardware security modules (HSM). Also, employees had to be educated. Procedures for key exchange had to be described and a policy and practice statement was developed. Costs all together were several hundred thousand euros, according to SIDN (Interview SIDN).

With the signing of the Top-Level Domain .nl in 2010 by the SIDN it became possible for registrars to issue signed domain names. SIDN supported registrars in adopting DNSSEC in a family and friends program, started in 2012. Several partners engaged in implementing DNSSEC worked together in a DNSSEC platform. This included partners like PowerDNS and NL net labs, that worked on open source software to support DNSSSEC. This resulted in an open source software solution for free available for a registrar to implement DNSSEC. Also, early adopters that were engaged in developing a safer Internet joined, like SURFnet. SIDN also employed a consultant that was available for registrars to solve problems. (Interview SIDN)

At the start of the adoption process bogus DNSSEC domain names caused serious problems. If a signature is not validated (for instance because it is expired) a website cannot be reached by a visitor that uses DNSSEC enabled validation. This causes problems for ISPs that provide validation. The website with a bogus domain name cannot be visited by someone who uses DNSSEC enabled validation, but can be reached by regular validation. For the average user, the 'fault' is caused by his access provider. This leads to many phone calls to these ISPs. Since the average costs of a phone call to the helpdesk is according to the SIDN about € 50, this is very costly for ISPs. (Interview SIDN)

On top of that, it also damages the reputation of an ISP. For a company like BIT that was engaged in the Friends and Family program of the SIDN this was quite an issue. BIT started validating DNS answers in the beginning in 2011. At the start, there were on average three calls a day, that sets the costs for an ISP for validating DNSSEC at approximately € 3 k a month, according to BIT (Interview BIT). It is obvious that this problem needs to be tackled before other ISPs can be convinced to turn on validation.

SIDN reacted on this problem by implementing a monitor program to reduce false signatures. Registrars that use bogus signatures were notified. Bogus domain names can be caused by wrong or expired signing keys, but also by a moved domain to another provider. According to the SIDN, the program was effective in reducing the number of bogus domain names from a couple of thousands to a couple of hundred (out of approximately 2,7 million signed domains). SIDN is also working on new software, that enables to implement changes in the zone file real time (instead of half an hour, that is currently the case). (Interview SIDN)

Next to this platform, the SIDN introduced a stimulating program to encourage the implementation of DNSSEC. Although not complicated, support for technical employees of registrars proved helpful. The SIDN offers a schooling programs for technical support of registrars. Also, registrars get € 0,28 discount for a properly signed domain on their contribution of € 3,40 a year. This is especially attractive for larger ISPs that sign domain names sometimes with thousands in one time. Based on a statement by the SIDN, the program has cost several millions between 2012 and 2017 (Interview SIDN).

Another part of the SIDN stimulating program is the Registrar Scorecard (RSC). This is dashboard designed for the registrar, set up to improve the quality of the .nl zone. The RSC consists of four criteria,

active use, contributions (where the discount is considered), actual contact data and security. The dashboard triggers awareness of quality, for instance validation errors. The RSC can also be used as a benchmark by registrars. Scores are available for each criterium. The RSC is currently used by 350 registrars. Goal is to raise awareness for security issues, where ISPs usually have a long list of deployment issues, according to the SIDN. (SIDN, 2017f)

2.3 The role of ISPs in DNSSEC adoption

The adoption of DNSSEC depends on an eco-system where several players must interact. Next to the SIDN ISPs play an important role in this. ISP is a collective noun for different roles, that need to be distinguished. On the one hand, there are ISPs that offer domain names (registrars), usually in combination with hosting services and e-mail. These are usually smaller companies (10 – 20 FTE). On the other hands there are access providers, that in many cases offer a wide range of services next to access. There companies are mostly bigger (around 1000 FTE). The focus of these companies is primarily on main stream products. These roles need to be distinguished, because DNSSEC implementation implies different consequences for hosting and access providers. It is important that all actors support the solution, one missing part of the chain will reduce advantages to zero.

2.3.1 ISPs: hosting providers

Investment costs for hosting providers can consist of new infrastructure, new software or working hours and education of employees. In many cases no investment in new infrastructure is needed, because of over dimensioning, according to hosting providers (Interview InterNLnet, BIT). There is open software available for DNSSEC, provided by NLnet labs and PowerDNS. Sometimes hosting ISPs need to invest to be able to adopt the open source solution (Interview InterNLnet). A hardware security module can be used for key management, but this is not necessary. Main investments regard working hours of employees. In some cases, employees have to be educated. Especially in large organisations procedures have to be adjusted, that are main contributors to (expected) investments. This based on an estimation by a somewhat smaller ISP (40 FTE) (Interview InterNLnet).

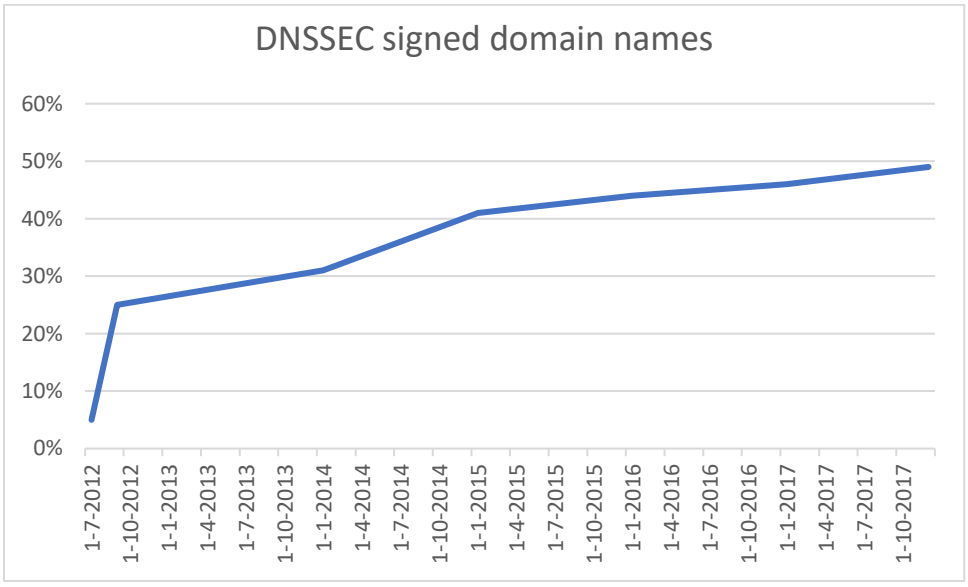
Enabling hosting is somewhat more complex than validating DNSSEC[31]. The expertise needed for DNSSEC hosting is often not present at ISPs. This mainly because this knowledge is more remote from the core business of hosting services. For this reason, SIDN has engaged a consultant that can help hosting companies to implement DNSSEC. The presence of this consultant sometimes is enough to get a company started. For signing and hosting provisioning systems need a software update. Usually it takes a couple of weeks to implement this. It also depends on the software architecture. In many cases no infrastructure investments are needed. The average costs for implementing DNSSEC for hosting providers are estimated by the SIDN around € 3 – 7 k (Interview SIDN). ISPs as InterNLnet indicate the same figures (Interview InterNLnet). According to the Internet Society experienced system administrators should be able to do the initial deployment in about a week.[32] As discussed in the introduction, it should be noted that statements and investment numbers are provided by

[31] There are adapters available like Plesk. Plesk is a web application to operate websites, including a web interface that can be configurated. Not only the webserver itself, but also accompanying services like e-mail accounts.

[32] Internet Society provides an instruction how to do this ("Deployment Guide: DNSSEC for Internet Service Providers (ISPs) | Deploy360 Programme," 2017)

stakeholders that support DNSSEC. It could be that these figures deviate (higher investments needed) if the research is extended to stakeholders that do not support DNSSEC.

Due to the SIDN 'friends-and-family' program targeted at the registrars, the number of DNSSEC domains rose quite fast to approximately 25% at the end of 2012 (SIDN 2017; 5). Large registrars signed their domain names sometimes with more than 100.000 at once. As a result, the Netherlands is doing reasonably well with 49% signed domain names (SIDN, 2017a). Worldwide this is much less, only 3% of the domain names are DNSSEC signed. But after this rapid start the adoption pace somewhat declined. (SIDN 2017b).[33]



Graphic 1. Number of DNSSEC signed domain names as percentage of total domains (SIDN, 2017g)

There are several reasons for the retarding adoption pace. For the SIDN, there are two main causes. First, a lot of IT is being outsourced. Most IT-infrastructure is located outside the Netherland, quite often also outside of the European Union. Companies like Huawei offer for instance datacentres, their main office is in China. Since the worldwide adoption of DNSSEC is very low, it is not very interesting from a business point of view to support DNSSEC hosting. Second, the implementation of DNSSEC is hampered by customers or businesses who arrange their own DNS server. This can be private customers, but also businesses. For these not professional parties it is difficult to arrange DNSSEC themselves. In many cases they do not have the knowledge to do this on their own.[34] (Interview SIDN)

Also, ISPs have quite often a lot of other security issues to tackle. The most urgent problems will be fixed first. From a competitive viewpoint, it is not very interesting to invest in security. As one

[33] Still, DNSSEC adoption is with Sweden (comparable adoption levels as in the Netherlands) among the highest in the world. (Chung et al., 2017)

[34] Of course, it is possible for company of home networks to maintain their own DNS infrastructure. But the adoption of DNSSEC for these networks requires quite some skill. For this reason, SIDN offers a solution to switch validation on for home networks. This can be done with the Valibox. If the Valibox is connected to the home network, it will behave as a Wifi-accesspoint with an own local Network Address Translation (NAT), that uses DNSSEC-validation.(SIDN, 2017h)

interviewee put it, 'too much security is a competing disadvantage'. (Interview InterNLnet) As is discussed in the next chapters, there are many reasons for the slowing down growth of DNSSEC signed domain names.

2.3.2 ISPs: access providers

Next to registrars and hosting providers there are access providers, that validate DNSSEC answers provided by the nameservers. Access providers are in general larger organisations (on average 1000 fte), usually with quite some technical knowledge. Implementing validation is not very complex. In the case of XS4all, this was implemented in four weeks by two employees, according to the SIDN (not full time). (Interview SIDN)

Sometimes investment in new hardware is needed. In the case of a large ISP there is also a large resolver infrastructure, new hardware can be costly. According to ISPs new hardware is not strictly needed to implement DNSSEC. In many cases infrastructure is over dimensioned and the larger DNSSEC queries cause no problems (Interview SIDN, BIT). Most of the effort to adopt DNSSEC is about aligning (new) processes within in the organisation, according to an ISP. For instance, about the downtime of DNS servers (Interview InterNLnet).

Most important access providers like KPN and Ziggo (together 80 – 85% of the market[35]) both do not provide DNSSEC. Only some smaller providers like BIT or XS4all do provide DNSSEC validation. There are several reasons for this. First, adopting DNS for large access providers requires a substantial investment (€ 200 – 300 k), based on estimations by the SIDN and an ISP (Interview SIDN, InterNLnet). Second, because of bogus domain names websites can get inaccessible of their end-users, while other providers do not suffer from this problem. As demonstrated earlier this problem has largely been solved, but DNSSEC still is perceived as a risky and complex solution, according to the SIDN (Interview SIDN) Third, access providers have little interest in providing DNSSEC.

So it is no surprise that the current level of validation in the Netherlands is at the moment approximately 22% (APNIC, 2017b). In countries like Norway (78%) and Sweden (74%) this is much higher.

[35] According to recent figures the market share of Ziggo slightly increased with 0.3% to 40,7%. KPN lost 0,1% to 41,7%. Both telecom providers compete for years in a shrinking market. (Emerce, 2017)

Participant	Role	Key facts
Registry [36]	- Trust anchor - Zone operator	- Lead-by example - ICANN 2014: obligation to implement - Implementation costs € 200- 400 k - Offering help to registrars - Several millions for registrar program
Registrar + hosting/ISP	- Issuing domain names - Signing domain names - Hosting nameservers	- Few incentives to implement DNSSEC - *One-time* investment, ca € 3 – 7 k - HSM € 50 k (optional) - Open source software - More complex than validation - Implementation in about 6 weeks - Small companies (10 – 20 fte) - Adoption level 49% (oct 2017)
Validating/ISP	- Validating DNS queries	- Implementing costs € 2 – 3 k - Large ISPs € 200 – 300 k (KPN, Ziggo) - No incentives to implement - Open source software - Suffer from bogus domain names - Implementation in about 4 weeks - Larger companies (1000 fte) - Adoption level 22% (oct 2017)
Registrant	- Consumer of domain names	- Mostly oblivious of advantages - Cost oriented - € 15-30 yearly for DNSSEC domain name (instead of € 4 for a regular one)
End-users	- User of websites and services	- Mostly oblivious of advantages - Suffer from negative externalities - DNSSEC not visible

Table 1 Stakeholders in the DNSSEC eco-system and their role in the Netherlands (based on Interviews with stakeholders).

[36] The registry is chosen as a starting point, the root is left out of scope.

2.4 Registrants

The market for domain names can be considered a commodity market. The registration of domain names usually is a low margin business, complementary to conventional ISP services like webhosting and e-mail. There are about 1350 registrars in the Netherlands, where a chosen domain name can be registered. A lot of registrars advertise with the price. Some registrars position themselves as safe and secure, usually with a small market share like XS4all[37].

Only a minority of the registrars offer DNSSEC signed domains[38]. Approximately one out of ten registrars present the DNSSEC as a default[39]. For a registrant, the challenge is to choose a good name that is available, not on meeting security standards. Security reasons hardly play a role in choosing a registrar. It is not easy to tell for a registrant whether a registrar offers DNSSEC[40]. In many cases price is the most important criterion. Large companies like KPN and GoDaddy offer domain names for a sharp price, but DNSSEC is an option that is cumbersome to activate (and comes with additional costs).[41]

Registrar	DNSSEC	Costs on a yearly basis[42]
On average	No	€ 4,-
KPN	No[43]	€ 3,96
GoDaddy	No[44]	€ 3,99
TransIP	Yes	€ 7,49
BIT	Yes	€ 15-20
InterNLnet	Yes	€ 24
XS4all	Yes	€ 30

Table 2 Costs for registration of a domain name on a yearly basis.

[37] See for instance https://www.xs4all.nl/pakketten/ondernemers

[38] The choice of a malevolent registrar can cause security problems that are very difficult to fix. In many cases essential security measures are not implemented by hosting provers. Registrants suffer from bad performance due to overloaded servers. This might seriously harm the reputation of a business. (TechRepublic, 2009)

[39] The SIDN offers an overview, where registrars can be selected that offer DNSSEC (SIDN, 2017g) Slight changes may occur due to different moment of access.

[40] Ibidem.

[41] The largest registrar in the world GoDaddy is also one of the cheapest.

[42] Retrieved from prices as presented on websites, https://www.kpn.com/zakelijk/domeinnaam.htm https://nl.godaddy.com/,https://www.transip.nl/domeinnaam-extensie/nl/ https://www.xs4all.nl/service/diensten/hosting-en-homepage/bestellen-en-ontvangen/wat-is-een-domeinregistratie.htm and interviews (BIT and InterNLnet), accessed Oct 23 2017. Temporary price cuts are left out.

[43] Optional use of DNSSEC additional costs € 20 per year.

[44] GoDaddy offers a 'premium package' that does include DNSSEC, costs $ 35 per year.

Costs differences between a regular and a signed domain are considerable. The largest registrars do not offer DNSSEC, and sell domain names for a low price. This can be caused by unawareness of registrants for advantages of DNSSEC signed domain names. But even if registrants are aware of this, and consider DNSSEC an advantage in their case, it is not very likely that they choose this (much) more expensive option. The price is much higher, and it is not the registrant, but the end-user who profits from a more secure domain name. It is also possible, that the DNSSEC solution is simply not considered a suitable solution for the registrant.

For a medium sized bookselling company that recently rebuilt the website Internet security issues are hard to assess. One of the challenges the company must deal with is how to determine the applicable standards. Establishing the appropriate risk appetite for the company and accompanying mitigating measure is very time consuming. This issue does not concern the core business of the company. The company was only once a victim of ransomware. Because there were backups, this had only a limited impact. The company is not confronted with leakage of (sensitive) customer data or other more severe cybercrime. (Interview Donner)

For the adoption of Internet security standards, the company had to rely on advice of the vendors. Https is part of the proposition, while DNSSEC is not. It was difficult for the responsible employee to determine what requirements had to be met. He was not acquainted with DNSSEC, like he is with https (the use of https is visible in the browser).[45](Interview Donner)

There are other incentives that push the use of Internet standards. Donner uses a newsletter to inform customers about new developments. Anti-spam filters used by Google are getting better, and Donner had to prevent the newsletter to end up in the spam filter. Although Google and other ISPs are not open in the way they establish if an email is spam or not, it is quite likely that Internet security standards like SPF and DKIM play an important role in this (for instance confirmed by Logius architect, (Interview Logius)). For this reason, Donner uses these standards on advice of the supplier. This to prevent the newsletter ends up in spam. (Interview Donner)

2.5 End-users

End-users are a large and diverse group, that range from individual users to small and large companies. For our end, this group is not segregated. One of the main difficulties of DNSSEC is that it is hardly visible for the average end-user. End-users expect security to be taken care of by suppliers, or included in a software update. An end-user must install a plug-in in a browser of use a tool as internet.nl to see whether DNSSEC used or not, this while many icons are confusing. So, just like in many other cyber security cases a clear majority of end-users is oblivious[46]. In the case of phishing, an end-user has to rely on his spam filter (and common sense). With the increase of standards and better spam filters, end-users can profit from a better security. This is also the case for (SME) companies, although they are in a better position to defend themselves against these threats.

[45] As recently announced by the department of Economic Affairs a new institute will guide SME companies in increasing cyber security measures. (Rijksoverheid.nl, 2016b)

[46] In general the awareness for cyber security risks is already low, see for this Alert online (Alert online, 2016)

2.6 Analysis

DNSSEC is a new solution that is adopted especially by tech-savvy ISPs and some other forefront runners[47]. Both access and hosting providers are in a good position to increase the security of the network. Investments in security are based on a balanced outcome of costs and benefits. Since there are not much known cases of DNS abuse, the benefits of investment are not clear. Also, effects of unsecured domain names are not borne by these ISPs, but by end-users. This can be considered a *negative externality*. All together it is very difficult to present a positive business case.

Another factor is knowledge. As Rogers points out, innovation creates uncertainty in the mind of potential adopters (Rogers, 2014; 13). For a registrant or and end-user it is not easy to see if DNSSEC is used. This limited visibility causes *information asymmetry*. Only with tools like Internet.nl or browser extensions as there are for Firefox or Chrome it is possible to see if DNSSEC is used.

For hosting ISPs (and registrars) the adoption of DNSSEC usually takes about six weeks to implement. These companies in general are smaller, and more often lack the knowledge to implement it. Adopting DNSSEC is also more difficult for hosting than for access providers. The SIDN support and incentive program to support the adoption of DNSSEC by hosting providers is partial successful. On average about 49% of all domains are DNSSEC signed. According to the SIDN, due to outsourcing and privately-owned DNS servers, further adoptions growths only slowly.(Interview SIDN)

Domain names can be seen as a commodity, where a registrant usually choses the cheapest. The unwillingness of a registrant to pay for a DNSSEC secured domain can be considered an example of the 'tragedy of the commons'. Actors that pursue their own interest neglect security as a common good (Anderson, 2001; 1).The registrant is willing to pay for a regular domain name, but additional costs for DNSSEC are not acceptable. It is also possible that registrants consider DNSSEC not relevant or cumbersome, given their risk profile.

Next to the higher price, only a minority of the registrars offer DNSSEC. According to the SIDN, it is very difficult to hold a registrar liable for missing Internet security standards (Interview SIDN). The registrars that do offer DNSSEC indicate that a minority of the registrants ask for DNSSEC. Those who do are more often (semi-) public institutions. A company like BIT that offers DNSSEC is a small innovative business, that is positioned in the high-end market. The company's core business is to build platforms, and domain names come are a prerequisite to do that. Since the costs for a domain name can be neglected when a platform is built, the somewhat higher costs (€ 15-20 on a yearly basis) for a DNSSEC domain name are according to BIT not a problem. (Interview BIT)

For (large) access providers, investments for adoption are considerable (€ 200 -300 k), estimated by the SIDN (Interview SIDN). For an access provider, it is even harder than for a hosting provider to get a positive business case for adopting DNSSEC. Although problems with bogus domain names have diminished, DNSSEC is still perceived as a complex solution. For ISPs, availability of service is key for the end-user. The risk of a website that becomes unavailable for their end-user is a worst-case scenario. All together access providers have no reason to adopt DNSSEC. On the contrary, access providers can only loose by adopting DNSSEC.

[47] According to York the adoption of DNSSEC is typical for early stages of deployment of new technology. (York, 2012)

These differences between hosting and access providers are clearly reflected in adoption levels (49% signed domain names, against 22% validation).

2.7 Conclusion

The DNS is a key component in the TCP/IP stack, providing a decentralised database of connections between (human readable) domain names and corresponding IP addresses. It is relevant to secure this protocol, to protect the 1.) authentication and 2.) integrity of data. This for instance in the case of e-mail security. In combination with other standards like STARTTLS and DANE it is possible to prevent e-mail against eavesdropping. Drawbacks of DNSSEC are the possible negative influence on availability, and increased vulnerability for a DDoS attack.

A signed top-level domain as provided by the registry is a prerequisite to issue DNSSEC signed domains by the registrar. The registry (SIDN) deploys several activities like providing knowledge and open source software to encourage registrars to adopt DNSSEC. A monitor program has limited the number of bogus domain names, and with the Registrar scorecard registrars can monitor the progress of their organisation. There is also a discount for the contribution for a signed domain of € 0,28, especially of interest for larger registrars operating domain names (Interview SIDN).

ISPs deliver many different services, that need to be distinguished. There are registrars that register domain names, usually in combination with hosting services and e-mail. According to the SIDN, supporting DNSSEC requires a limited investment in time and money. To adopt DNSSEC for a hosting party costs are estimated by the SIDN and BIT about € 2-3 k and a limited number of working hours of employees. (Interview SIDN, BIT)

Validation of DNSSEC signed domain is just as important as hosting. Access providers like KPN and Ziggo suffer from bogus domain names, that negatively influences the availability of websites for their customers. Although this problem has diminished over the last years, DNSSEC still is perceived as a cumbersome solution. There is very little to gain for access providers, and large ISPs are confronted with considerable costs to adopt validation. So, it is not surprising that these ISPs do not support DNSSEC.

Chapter 3 Regulating adoption in the (semi-) public sector

As shown in the previous chapter the further adoption of DNSSEC is not warranted. For policy makers, this is a point of concern. Questions is if government intervention can increase this pace. To analyse this at first the current comply-or-explain regime is described. Next, the Wet GDI is discussed. Conclusions are validated by interviews conducted with stakeholders. This analysis explains why a relatively high number of 59% of the domain names are DNSSEC signed.

3.1 Addressing market failures

One of the characteristics of security investments is that all participants in the ecosystem profit from it. It is not possible to exclude a participant from these benefits (non-excludable). If someone enjoys the benefits of this investment, these advantages can still be used by someone else (non-rivalrous). These characteristics cause that it is difficult to invest to offer these services. Since the decision to invest is made by market players, this is not the social optimal level. Cyber security has strong characteristics of a public good. (Bauer & van Eeten, 2009; 717)

The adoption of DNSSEC is also growing at a slow pace due to market failures. *Misaligned incentives* make it hard for ISPs to invest in Internet security standards. ISPs that invest in security, will not profit from it. Due to *misaligned incentives* only, a limited number of registrants are prepared to pay an additional € 5 – 20 for a secure domain name. It is not the registrant, but the end-user who profits from a secured domain. It is also possible that a registrant decides on a risk based approach that DNSSEC is not a reasonable mitigating measure.

One could reason that public good characteristics and market failures legitimise government intervention. As Minister Kamp states in a letter to the Parliament adoption of Internet security standard is of public interest (Ministerie van Economische Zaken 2017, 1). Limited adoption causes damage to the interest of citizens, companies and other governments. All (semi-) public institutions should adopt these standards. (Ministerie van Binnenlandse Zaken, 2017b; 7)

3.2 Comply-or-explain

Forum Standaardisatie plays a central role in encouraging interoperability and security in the (semi-) public sector[48]. By using Internet security standards (including DNSSEC) as a (semi-) public institution, it is easier to exchange information with citizens and other parties. This should lead to higher quality of digital services and more efficient operation of ICT systems and reduction of costs. This in line with the Cabinet's mission to create a right for citizens to do (safe) digital business with the government. (Ministerie van Binnenlandse Zaken, 2015; 1)

The comply-or-explain policy is aimed at market development, legitimation and practical experiments. To do this the Forum Standaardisatie maintains a list of (Internet security) standards, that are directed towards the promotion and adoption of these standards. For all organisations within the (semi-) public sector, there is a 'comply-or-explain' regulation. An instruction how to adopt standards is noted in the *Rijksbegrotingsvoorschriften* of the department of Finance (Ministerie van Financien, 2017). This instruction includes a way of working for (semi-)public institutions, for the purchase of new ICT products. This entails that organisations are supposed to include these standards when ICT systems are purchased over a value of € 50 k. (Ministerie van Economische Zaken, 2008)

[48] The public sector is defined as governments (national, provinces, water boards, municipalities), semi-governments (UWV, SVB) and private institutions with a public task (hospitals, schools and universities).

There is room for an organisation to deviate from this rule. This is for instance the case when there are no suitable standards available. When this is the case, an explanation should be included in the annual report. Within the program there is also room for experiments by research on the area of interoperability and adoption strategies. (Poel, 2017, 75) Local governments have committed themselves to this policy, based on the Bestuursakkoord 2011-2015.(Rijksoverheid.nl, 2011)

Any organisation can suggest a standard to be included in the comply-or-explain list. If a standard meets the criteria, a procedure can be started to add the standard to the list. According to these criteria a standard must be applicable for electronic data exchange between (semi-) governments. It should contribute to interoperability of the ICT systems and must not depend on specific vendors. Also, there must not already be a legal obligation to use the standard. (Forum Standaardisatie, 2017b)

Next to formulating open standards, it is equally important that these standards are incorporated in business policies. These policies should include implementation of the standards in specific systems and processes. Most policies comprise financial and procedural requirements, but quality should also be part of it. The use of open standards are part of this quality aspect of ICT. (Forum Standaardisatie, 2017b)

There are several relevant policies of which open standards should be part of. In most organisations, there are several IT governance processes implemented. Mostly these are compliance management, IT policy, architecture, portfolio management and buying processes. The use of open standards has to be part of these policies. For instance, the check of standards that are on the compulsory list can be part of compliance management. In architecture documents should be specified which standards fit within the enterprise architecture. Based on the plan-do-check-act cycle[49], these instruments can become part of an ongoing process of improvement. (Punter, Verhoosel, Folmer, & Luttighuis, 2010)

The (enterprise) architect has an important role in this process. It is the responsibility of an architect to determine what standards are relevant for a project. The applicable standards are listed in the Project Start Architecture (PSA). Employees from the buying department decide based on this advice what is relevant to ask from a ICT vendor. The requirements must be specified in terms and conditions. Forum Standaardisatie offers a guideline for buyers that helps to formulate the terms and conditions. (Forum Standaardisatie, 2008)

[49] Known as the Deming-cycle. The PDCA cycle is a model for continuous improvement that consists of four iterative steps (plan, do, check, act).

DNSSEC requirements Forum Standaardisatie	
Functional area	The signing and registration of Internet domain names. The registration obligation is only applicable, if a signed domain can automatically be requested at a registry (SIDN for .nl). Also, the validation of translation of domain names to Internet addresses and vice versa (validation enabled resolving). Validation is not required for systems that are not directly connected to the Internet (for instance clients within LAN networks and internal DNS systems).
Organisational area	Governments and organisations in the (semi-) public sector.

Table 3 DNSSEC requirements as formulated in the list of compulsory standards (Forum Standaardisatie, 2017a)

One of the problems with this list is to determine exactly what a (semi-) public institution has to do. On the one hand, a definition should be short and clear, on the other hand it should be technically correct and complete. There is quite often discussion about the functional working area, more than about the organisational area. Because this part determines what governments have to implement this is important. The definition (including other standards) is currently under review (Forum Standaardisatie, 2017c).[50] Basically there are two elements in the description, the signed domain names and the validation of the DNSSEC answers.

The comply-or-explain program is executed under supervision of the department of Economic Affairs. This is the responsibility of the section Regeldruk and ICT-beleid (R & ICT). The department of Internal Affairs also contributes to this program. One instrument that can be used is the relative number the standards were requested during tenders. Buying departments of governments are supposed to request from their suppliers the use of open standards when systems over € 50 k are bought. According to these figures open standards are increasingly requested. The Forum Standaardisatie has developed a guide how to do this. (Poel, 2017)

[50] A recent proposition entails 'DNSSEC should be applied to all government domain names and to the DNS resolvers, to supply all clients validated DNS answers'. Also, this definition is troublesome, because validation should be executed within a trusted network. It is not desirable to use Google public validating resolvers, where validated answers are unprotected exchanged by the Internet before they are used by clients. The expert committee advises to leave this part out because of readability reasons. (Forum Standaardisatie, 2017c)

	2014	2015	2016
Completely/most important requested	14%	14%	44%
Partly requested	28%	50%	27%
Not requested	59%	29%	29%

Table 5 Open standards requested during tenders (Poel, 2017, 77)

There are also other instruments that regulate the use of Internet security standards. The National Cyber Security Centre publishes influential papers, for instance *Beveiligingsrichtlijnen voor webapplicaties*. Assessments are based on these documents, that are obligatory for a government to conduct while using DigiD. The requirements are formulated in *Handreiking DigiD assessments V2.0* by the organisation of IT auditors, the Nederlandse Orde van Register EDP-Auditors (NOREA). As a part of this, the *Handreiking* states that the use of DNSSEC is compulsory.(NOREA, 2016)

These audits are quite a forceful instrument to push the use of DNSSEC. A DigiD audit is compulsory after two months when the application is available for public (production stage). DigiD is used by approximately one out of ten websites. The use of DNSSEC is also compulsory for eHerkenning (a means for entrepreneurs to use services from the government). Since these requirements are not audited, this is a much less forceful instrument.

3.3 Wet generieke digitale infrastructuur

The Forum Standaardisatie each year publishes a report, in which the progress of the adoption of standards is evaluated (based on statistics provided by the SIDN). These figures show that the number of DNSSEC signed domain names used by (semi-) public institutions are gradually growing.[51] (Rijksoverheid.nl, 2016a)

Standard	On the list since	Use by (semi-) public institutions		Development
		Total	Central	
DNSSEC	2012	45%	59%	Growth from 25% (2015) to 45% (2016)

Table 4 Number of (semi-) public institutions that use DNSSEC signed domains (Korpel & Vreuls, 2016, 25)

A recent evaluation states that it is hard to establish the effectiveness of the open standards program. Because of legacy problems and many ongoing projects, the adoption of open standards is not so easy. According to a recent evaluation of the R & ICT section (department Economic Affairs) there are

[51] DNSSEC validation within the sector (second part of the standard) has not been measured.

persistent problems that come along with the implementation, such as doubts about adoptability, complexity of use, and insufficient knowledge of the standards.(Poel, 2017; 77)

According to policy makers the adoption pace is too slow and has been reason to design an obligation for (semi-) public organisations to use Internet security standards. This obligation is formulated in the Wet GDI, that stipulates conditions, in which adoption of a standard is necessary. The proposal consists of a rule to constitute Internet security standards by *Algemene Maatregel van Bestuur (AMvB)*, so it can be established by a minister without consulting the parliament. This makes it easier and faster to add (or remove) required standards. (Ministerie van Binnenlandse Zaken, 2017b)

The Wet GDI (art 2 second provision) offers a ground to appoint a standard by AMvB, that is compulsory to implement. Standards that are appointed by AMvB will be removed from the 'comply-or-explain' list. The Forum Standaardisatie will be responsible for the consultation process, before a standard can be determined. The use of these standards will be monitored each year. (Ministerie van Binnenlandse Zaken, 2017b)

This procedure will not be applied for all standards. For some standards, the comply-or-explain policy will be sufficient. This contains the currently practiced mixed approach of an obligation to explain if an organisation deviates from the norm, in combination with instruments that enhance the visibility of the use of Internet security standards. For some standards this approach is insufficient and an obligation will be introduced for all governments to apply these standards. (Ministerie van Binnenlandse Zaken, 2017b)

The implementation by AMvB complies with the way of determining standards by the Forum Standaardisatie. A standard on the comply-or-explain list has an organisational working area and a functional working area. The way of determining a functional working area is adopted from the Forum. This to make sure that everyone can express their opinion about introducing an obligation for a certain standard. This also goes for the organisational area, that is determined per standard. This including a date of introduction of the obligation.

A standard can be appointed if this is 'necessary and proportional', regarding 'working, security, reliability and efficiency of electronic traffic'. It also can be compulsory to implement, because of international law. This is for instance the case with Web guidelines, while there is a European regulation regarding the access of websites and mobile applications of the government. Since the Wet GDI is still in preparation, for most standards (including DNSSEC) it is not yet clear which one will be appointed. (Ministerie van Binnenlandse Zaken, 2017b; 1)

The Wet GDI is designed by the department of Internal Affairs, in cooperation with the Economic Affairs department. This relationship is sometimes difficult because of divergent paradigms. The department of Economic Affairs is usually reluctant in adopting a large role for the government. Only market failures legitimate intervention of the regulator. In the reasoning of the department of Internal affairs the state has a well-defined role in providing security (and reliable access means, which is the largest part of the Wet GDI). (Ministerie van Binnenlandse Zaken, 2015)

3.4 Adopting DNSSEC

In many cases architects play an important role on advising on the adoption of Internet security standards. Within several public institutions formats are used for architecture documents. In these documents, the comply-or-explain-list is a compulsory part, as indicated by the Logius as well as the

Dictu architect (Interview Logius, Dictu). The requirements of the architecture document are the basis for the application that is built by a supplier. So, the architect is quite a central figure in implementing cyber security measures.

For DICTU as the ICT supplier of the department of Economic Affairs the comply-or-explain list is important as a reference. The list puts the topic on the agenda. Internet security standards listed in the comply-or-explain-list have been added to the Project Start Architecture (PSA). The obligation to explain if standards are not used makes the architect start questions. The presence of several versions of Internet security standards makes it possible to be a bit flexible. If a TLS 1.2 version is not available, the TLS 1.1 can be accepted in certain cases. The comply- or- explain list increases the attention for the topic. From the client side, the awareness for standards is usually limited. Only in a few cases (internal) clients ask for government standards, according to DICTU. (Interview DICTU)

For the architect, the work is done when the PSA is finished. The supplier is responsible for the way the application is built. The PSA is used to specific the client's needs (functionalities), so the supplier can calculate costs for offering. Security is often regarded as 'nice to have'. Many developers are not familiar with security requirements. Also, in many cases security requirements are left out because the clients consider these too expensive. Anderson referred to this phenomenon as 'we'll ship it on Tuesday and get it right by version 3'. (Anderson, 2001; 2)

Another factor in deciding on security investment is infrastructure. There are solution architects and infra architects, who decide on infrastructure investments. This is important for DNSSEC hosting. Usually infrastructure is used for many applications, according to DICTU. So, if this infrastructure does not support DNSSEC hosing, the adding of a new application will usually not lead to buying new hardware. If this hardware is recently purchased, this is also not very rational. (Interview DICTU)

In the case of DigiD the Logius architect indicates that the comply-or-explain list is strongly supported by the management. Background for this are security incidents with DigiD, that caused a lot of media and political attention. Although several incidents were not technically related, this increased the awareness of risks connected to the use of a public ID. When DNSSEC was added to the comply-or-explain list, this triggered Logius to implement DNSSEC for DigiD. (Interview Logius)

As demonstrated earlier, the implementation of DNSSEC shortly after introduction in 2010 was complicated. This not only because of the bogus domain names, that cause validation problems. Suppliers of Logius did not find it easy to implement DNSSEC. Basically because of DNSSEC is not off the shelf available. Tools the suppliers use, had to be adjusted to support DNSSEC. To do this, processes had to be changed and operators educated. This also affected the time for Logius, until the solution was available. In total cost for adopting DNSSEC by Logius were € 30 k, a considerable amount. (Interview Logius)

The distribution of (signed) domain names since then has been changed. For efficiency and policy reasons the Dienst Publiek en Communicatie (DPC) of the department of General Affairs is now responsible for issuing domain names for all central governments (water boards and municipalities excluded). This makes it easier to comply to communication guidelines, but also on security policy. For instance, a newly issued domain name is default blocked for e-mail facilities. Only if applicable Internet security standard such as SPF and DKIM are used, it is possible to use a domain for e-mail, according to DPC. (Interview DPC)

To do this DPC is able to act as a registrar. DPC is the domain name holder, under the label *Rijksoverheid*. This for .nl, but in some cases also for .com, .tv and other extensions. About 80% of all domain names used by the government is operated by DPC, in total around five thousand. Some large organisations like the *Belastingdienst* operate their own domain names, as an interviewee indicated. (Interview DPC) Also, for central governments it is still possible to obtain a new domain name without DPC, but this is getting more difficult.

From this central position, it is easier to operate according to Internet security standards like DNSSEC. A standard policy is, that all newly issued domain names are DNSSEC compliant. The older domain names are being adjusted to support DNSSEC. This is done by formulating several criteria. If a website is for instance used for transactions, has a lot of visitors, is used for e-mail or by the secret service it is prioritised. Currently a tool is being developed to be able to monitor the number of DNSSEC signed domain names operated by DPC. (Interview DPC).

To be able to execute this task, the DPC maintains a network of employees within the Rijksoverheid, called *liaisons*. These liaisons are well informed about the security policy of DPC, and explain this to their customers. There are about 75 liaisons engaged in the network of DPC. Liaisons are responsible for compliance of their organization. It is not allowed to register domain names or prolong certificates that liaisons are not aware of. It is also convenient for clients (i.e. employees who want to register a new domain name) to use liaisons because in this way they can make sure websites or other applications are compliant, according to DPC. (Interview DPC)

3.5 Analysis and policy options

It may be difficult to establish the effectivity of the comply-or-explain policy, in combination with other regulation as audits and the DPC policy there are all together quite a lot of checks and balances to make sure that domain names are signed within the (semi-) public sector. There is diminishing room to deviate from these rules. These factors all together explain the rather high number of signed domains (59%) within the (semi-) public sector. Within the (semi-) public sector less risk can be accepted (for instance with DigiD). This makes it easier to finance security standards.

Goal of the Wet GDI is to accelerate the adoption of Internet security standards like DNSSEC by creating an obligation. This ‘when necessary and proportional’, and needed for ‘good working’. Setting and enforcing a security standard is quite an intrusive measure. Question is if this law is focussed (adoption in the (semi-) public sector is already high) and effective. As stated before, government regulation can be effective if well designed. To determine this principles of Lodge and Wegrich for good regulation are used. These are the following principles. (Lodge and Wegrich 2012; 54)

1. Proportionate
2. Accountable
3. Consistency
4. Transparency
5. Targeted

Two criteria are assessed in more detail. One is ‘proportionate’. Investments for (semi-) public organisations should be related to reduction of risks. According to art 2. of the Wet GDI a standard can be appointed by AMvB. All though this will only be done ‘when necessary and proportional’ and ‘needed for good working’, a standard can become de facto an obligation for all (semi-) public institutions. Once appointed, there is no room to deviate from the norm of adopting the Internet

security standard (such as DNSSEC) for targeted organisations. (Art 2 Wet GDI) (Ministerie van Binnenlandse Zaken, 2017b)

This principle is contrary to the risk oriented approach as common in cyber security guidelines[52] [53]. Key elements that need to be considered are context establishment, risk identification, risk estimation, risk treatment, risk acceptance and monitoring and review (ISO 27005). Risks can only be assessed at the level of a separate service, in the specific context (and not beforehand for the whole sector). Risk analysis consists of understanding the nature of the risk and determination of likelihood and consequences. The risks must be evaluated, for instance on basis of the strategic value. Then several options are available (acceptance, transferring, reducing or avoiding) for the owner to deal with the risk. (ISO/IEC, 2014; 8-9)

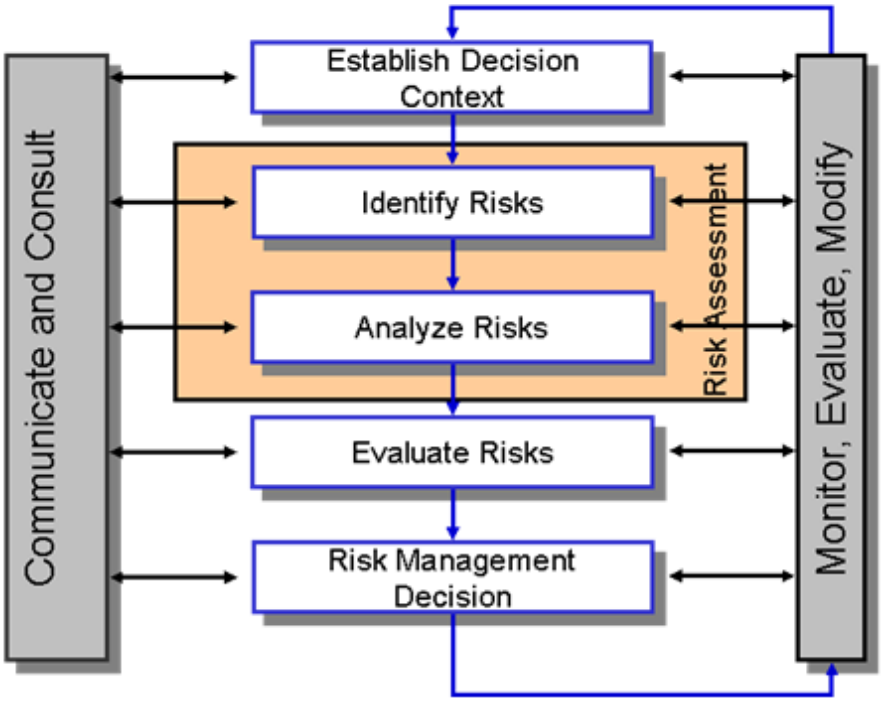


Figure 5 The risk management process according to ISO 27005 (ISO/IEC, 2014; 8).

According to interviewees an explicit risk consideration made by the client is at the heart of the decision to invest in cyber security solutions. For instance, for DigiD is was no problem to invest € 30 k in the adoption of DNSSEC (Interview Logius). On the other hand, where new applications are designed by DICTU it makes no sense to replace equipment or software just to support DNSSEC, if not needed for other reasons. A risk oriented approach is also used by DPC. The DPC maintains five thousand domain names, that do not all support DNSSEC. DPC has started to adopt DNSSEC for the most important domain names. Used criteria can be number of visitors, use for e-mail, transactions or used

[52] There are many cyber security guidelines available. There are differences between these guidelines, but are all based on a risk oriented approach. See for more detail for instance ISO 31000/27000 or NIST frameworks Only some basics of risk assessment are highlighted here, based on ISO 27005.

[53] This approach is opposed by U. Beck. In the article 'Living in the world risk society' he states that modern society has become preoccupied with risks. In his vision risks cannot be calculated or controlled. (Beck, 2006)

by the secret service, as indicated by DPC (Interview DPC). The use of Internet security standards like DNSSEC should be based on a risk assessment and on the organisations risk appetite.

The second criterium for good regulation that is discussed here is 'targeted'. Regulation must address issues to specific actors. If (legal) provisions are vague, no behaviour will change. The DNSSEC solution depends on both signing and validating DNSSEC answers. Both aspects are addressed in the definition of Forum Standaardisatie. But it is not clear if (semi-) public institutions validate DNSSEC if other systems are approached. In the yearly evaluation of the adoption of DNSSEC by the Forum Standaardisatie, this part is left out of scope. (Korpel & Vreuls, 2016; 25)

These metrics cannot be missed for several reasons. As described in the analytical framework regulation is about setting a standard, that can be monitored (Black, 2002; 26). Without metrics, it is very difficult to establish the effectiveness of the regulation. Also, security investment models heavily rely on metrics. Risks cannot be managed, until they are measured. (Böhme, 2010) (R. A. T. Moore, 2006)

In the Netherlands only 22% of DNSSEC answers are validated, while in Scandinavian countries this is around 70%. The Wet GDI is aimed at (semi-)public institutions[54]. In this definition, ISPs are not included. In the case of hosting (semi-) public institutions can act as a lead user. On the access side, this is much more difficult. Validation on the customer site is usually done by large access providers like KPN and Ziggo. These companies dominate the telecom market and do not offer DNSSEC. The regulatory regime for ISPs is very different from the (semi-) public sector, as will be discussed in the next chapter.

Although not watertight, there are several advantages connected to the current regulation (comply-or-explain, DPC, audits). There is room to deviate from the standard, if there are good reasons to do so ('proportionate'). It also addresses responsibilities to the right actor ('targeted'). In combination with the compulsory audits and the DPC buying procedures there are a several checks and balances, that explain relatively high adoption levels. More consequent monitoring could improve the effectiveness of this policy.

3.6 Conclusion

Since the adoption of DNSSEC is quite well incorporated in processes within organisations (architects/buying procedures, audits, DPC), there are a lot of checks and balances to make sure that DNSSEC is used. Since a risk based approach is at the heart of a security investment, the organisations risk appetite is also important. Governments tend to be risk avoiding, which makes it easier to finance additional security measures (as is the case with DigiD). These factors together explain the rather high number of signed domains (59%) within the (semi-) public sector.

[54] The (semi-)public sector is defined as governments (national, provinces, water boards, municipalities), semi-governments (UWV, SVB) and private institutions with a public task (hospitals, schools and universities).

According to the Cabinet the adoption of DNSSEC signed domain names is lagging. To accelerate this, the Wet GDI is in preparation. This law introduces an obligation for (semi-) public institutions to use DNSSEC by default. One of the criteria for good regulation is ‘proportionate’. But this law does not include a risk based assessment, as adopted in cyber security guidelines (‘proportionality’). Since the Wet GDI focusses on governments, the validation side (more worry some because large access providers do not support DNSSEC) is left out of scope (‘targeted’).

Chapter 4 Regulating adoption in the ISP sector

The ISP branch is a dynamic sector, that consists of many players with different roles. In this chapter at first some characteristics of the ISP sector are discussed. As a next step, the current regulatory regime for ISPs is analysed. The *Telecomwet* determines the leeway for market players. Then the impact of the Wet GDI is assessed. This based on interviews with stakeholders (ISPs). Other existing forms of collaboration with market players are also investigated, and alternatives discussed. A refinement of the regulatory regime can help to reduce market failures, like negative externalities and information asymmetry.

4.1 Characteristics of the ISP sector

Most companies that offer ISP services are privately owned and range from small to very large businesses. Due to network effects, the market for ISPs is highly concentrated. Because of these effects, a service gets more valuable if the service is adopted by more users. Since usually fixed costs are high and marginal costs low, adding users is very profitable. This mechanism makes it possible for a few companies to dominate the market. Some of the world's largest Internet Intermediaries are biggest firms in the world, like Google, Facebook and Microsoft (Michel J. van Eeten, 2008; 271)

ISPs play an important role in providing cyber security. ISPs have direct access to end-users, and often have access to valuable information about cybercrime, for instance about botnets. In many cases, end-users are oblivious of the fact that their computer is being abused by a botnet. According to Van Eeten, standardisation bodies and technical choices of ISPs have more impact than formal Internet governance strategies. This because ISPs have the resources, knowledge and capabilities to provide security for the end-user. (Asghari, van Eeten, & Bauer, 2016; 272) ISPs thus play a crucial role in aligning the costs of preventing cybercrime with the risk of becoming victim of this.

Security comes with costs, and it is economical rational to accept some level of insecurity. Question is whether costs and benefits are aligned with social optimum. Essentially there are three situations: 1.) no externalities 2). externalities that are borne by actors that can manage them 3.) externalities that are borne by actors who cannot manage them. A much-used example to demonstrate this effect is the financial sector. In the US, a bank is accountable for fraud. The US banks suffer from less fraud, while they invest less in security. A bank bears the costs of fraud, but is also in a good position to do something about it. Because of this, investments can be very efficient. (Anderson, 2001; 1)

The business case for investing in security by ISPs is complicated. An ISP is well informed and in a good position to increase the security of the network. But due to absence of outside pressure incentives for security are not strong. Effects of unsecured domain names are not borne by these ISPs, but by registrants and end-users. This can be considered a *negative externality* (B. Schneier, 2007). It can create a *moral hazard*, end-users suffer the consequences for a lack of investments. An end-user expects safety to be a standard, taken care of by the supplier. End users consider themselves to a certain degree responsible for online behaviour, but they perceive technical aspects of security as a responsibility of a software vendor, ISP or government. (Michel J. van Eeten, 2008; 52)

4.1.1 Hosting providers

ISPs conduct a wide array of activities, that can be categorized in hosting, access and others. Hosting providers are organizations that operate servers used by consumers to make content and services available to the Internet. Hosting ISPs are commonly somewhat smaller in size (10-20 FTE). Hosting

companies also offer additional services like datacentres, networks, platforms or manage online sales. These services are usually provided on a subscription basis.

Many companies that offer hosting services also act as registrar and provide domain name registration services. Domain name registration is a low margin business, sometimes domain names are even sold with loss to gain other assignments.(Michel J. van Eeten, 2008, 46-49) Usually the registrar just choses the cheapest vendor. There are some larger registrars, that provide domain names on a huge scale, like TRANSIP.

Hosting providers are an important actor in providing DNSSEC. SIDN has deployed several activities to make it easier for a hosting company to adopt DNSSEC. Due to the 'family and friends' program there is open source software available, that hosting providers can use for free. Costs of adopting DNSSEC are limited to working hours of employees, estimated by the SIDN around € 2- 7 k (Interview SIDN). This is a onetime investment for all domain names, with *high fixed and low marginal costs*. There is also an incentive arrangement, that entails a reduction of € 0,28 of the contribution of € 3,40 a registrar has to pay to SIDN (per domain on a yearly basis). (Interview SIDN)

This program proved to be partial successful. On average about 49% of all domains are DNSSEC signed. Most of the companies that offer DNSSEC signed domain are usually small companies, that also offer other services like platforms. Offering a DNSSEC signed domain name fits to a proposition in the more quality oriented niche market, or have (semi-)public sector organisations as client. These are companies like XS4all, BIT and InterNLnet. Large registrars (like KPN and GoDaddy) in general do not support DNSSEC.

In many cases hosting providers indicate that only a minority of their customers demand for an DNSSEC signed domain name, even if the provider does offer DNSSEC. (Interview BIT, InterNLnet). Because of this, the costs for ISPs to adopt DNSSEC may be larger than the benefits. So, each decision maker might wait for others to go first. Because of this, the problem looks like a prisoners dilemma. As a result, technology gets slowly adopted.(Moore, 2006; 4-5)

Another challenge for DNSSEC adoption is visibility. An end-user must install a plug-in in a browser or use a tool as internet.nl to see if DNSSEC is used (mostly only signed domain is shown, not validation). So, a clear majority of end-users is oblivious of the use of DNSSEC. Because of this *information asymmetry* it is hard to tell for and end-user whether DNSSEC is used. Most registrars sell domain names without DNSSEC, against the lowest price. This is difficult to compete with for a company that does offer DNSSEC. The market for domain names thus is a market for lemons (Bruce Schneier, 2007). As a result, bad products drive out the good. (Akerlof, 1970) As one interviewee puts it, 'you are being punished for (offering too much) security'. (Interview BIT)

4.1.2 Access providers

Another kind of ISPs are access providers. These ISPs provide end-users with a data connection to the Internet (physical transport). This access is needed for end-users to access or publish content online. An ISP can grant local or regional coverage to publish or distribute online content. Access providers are usually larger in size (up to 1000 FTE). Access providers include both cable and telecommunications providers, wired as well as wireless connections. In many cases service is bundled with telephone and television (triple play).

For access providers, the business case for DNSSEC adoption is worse than for registrars. Due to bogus domain names, websites may become unreachable, a serious issue while availability of services for the end-user is a main concern. Since a phone call to the helpdesk costs € 50 (estimated by the SIDN (Interview SIDN)), this can lead to considerable costs. Although this problem largely has been solved, DNSSEC is perceived as risky and complex. On top of that, for large access providers investment costs to adopt DNSSEC are considerable. So, it is no surprise providers like KPN and Ziggo do not support DNSSEC[55].

Availability of services also is a main concern for banks. In the case of a bogus domain name, the website of the bank can become unreachable, a serious issue for the bank. On the benefit side, there is not much to gain. A bank will only invest in security if there is a good reason to do so. Since there are not many security incidents related to the DNS, this is not the case. The problem is simply not serious enough (yet). An unwritten statement within the financial sector is that banks will not compete on cyber security. This often means that there is no urge to act, because competitors also do not act. Also, ICT services in the financial sector are relatively often outsourced abroad, and DNSSEC adoption worldwide is very low, according to the SIDN. (Interview SIDN)

Both hosting and access providers are in good position to increase security within their network. For hosting providers, it is possible to adopt DNSSEC against acceptable costs. At least, open source software solutions are available, that limit the necessary investments. But especially at the access side, there are several factors that hamper the adoption. If these factors are not mitigated, access providers will not adopt DNSSEC. To a somewhat lesser degree this is also the case for hosting providers.

These differences are clearly reflected in adoption levels (49% signed domain names, against 22% validation) (SIDN, 2017d). As explained in the (semi-) public sector chapter (chapter 3) risk appetite is an important factor in cyber security investments. These risks are generally lower for ISPs than for the (semi-) public sector. Partly because of this, checks and balances in the (semi-)public sector are absent here. In some cases, there are additional costs for a hosting ISP to adjust (open source) software to be able to use it for their own networks. (Interview InterNLnet)

Question is whether regulation can correct a negative business case, externalities and information asymmetry.

4.2 Regulation of the ISP sector

The ISP sector is regulated by the *Telecomwet.* This law entails several provisions about net neutrality, frequency policy, end-user rights, and in what circumstances the government can have access to customer data. It also includes a number of EU directives. Since the telecom sector is a very innovative and highly dynamic market, regulation is designed not to interfere with these developments. Because of this, the law focusses on general affairs and norms. The *Telecomwet* is designed as a *kaderwet*, that consists of a flexible framework that relatively easy can be adjusted to changing circumstances. The *Telecomwet* is enforced by Agentschap Telecom and the Autoriteit consument en markt. (Agentschap Telecom, 2017)

Most provisions of the *Telecomwet* are not relevant for this thesis. There is one article about security, Article 11.3, second provision. This article states that ISPs should adopt a suitable security level, that is proportional to the accompanying risk of personal data leakage from customers and users. To

[55] Both companies did not want to cooperate with this research.

mitigate this risk suitable technical and organisational measures should be taken. This to protect the safety and security of the offered networks and services. (Ministerie van Economische Zaken, 2017b)

These measures should guarantee that the security level is compliant with the risks that occur. One could reason that to protect these data, an ISP can be held to implement Internet security standards. If for instance no DNSSEC is used, it is possible (with spoofing) to acquire personal data from customers. In practice, this article is very difficult to use against ISPs, because it is hard to achieve consensus about the required level of protection. So, the chance that an ISP can be held liable in this sense is very small. For this reason this article is not enforced in this sense by the Autoriteit Consument en Markt. ("wetten.nl - Regeling - Beleidsregels informatieplicht voor aanbieders over internetveiligheid (artikel 11.3 tweede lid van de Telecommunicatiewet) - BWBR0033401," 2013)

The department of Economic Affairs is responsible for the regulation of the Telecom sector. Main task of the department is to encourage entrepreneurship and a strong international trading position. Market failures or system failures are seen as a legitimate ground for government intervention. The accent in policymaking lies on cooperation with companies and stimulation of innovating initiatives with all kind of instruments. The *Directie Telecom* within the department of Economic Affairs is responsible for the *Telecomwet*[56].

4.3 ISPs and the Wet generieke digitale infrastructuur

Although ISPs are out of scope of the Wet GDI, this law does affect ISPs, according to interviewees. As noted the Wet GDI can be considered an extension of the comply-or-explain-list as maintained by Forum Standaardisatie. The law introduces a possibility to appoint a standard by *Algemene Maatregel van Bestuur*, an example of *ex ante* regulation. A standard can be appointed if 'necessary and proportional', regarding 'working, security, reliability and efficiency of electronic traffic'. It is not yet clear what standards will be implemented based on an AMvB. This procedure will not be applied for all standards. For some standards, the comply-or-explain policy will be sufficient.

4.3.1 Hosting providers

For ISPs, the Wet GDI just as the comply-or-explain-list is of interest because (semi-) public institutions increase the demand of DNSSEC based solutions. Although still limited, ISPs notice a demand for DNSSEC caused by governments, that create a business case. (Semi-) public institutions act as a lead-by example, that create an incentive for hosting providers. This is still a niche market, where technological advanced companies offer secure solutions in the higher end of the market[57]. These companies usually provide complete solutions like a platform, with additional (secured) services like issuing of domain names and hosting. The somewhat higher costs for DNSSEC domain names and hosting are then taken for granted and part of the quality oriented solution, according to BIT. (Interview BIT)

ISPs do indicate that the effectivity of the law depends on enforcement. Just as the case with the comply-or-explain list, there are doubts if this is the case. ISPs indicate that in tendering the company with the cheapest offer usually gets the assignment. Offering businesses get away with vague promises

[56] Telecom is a different part of the department of Economic Affairs than the section in charge of the Wet GDI, art. 2 Internet security standards, called Regeldruk & ICT.
[57] In some cases these are small independent companies like BIT, but can also be a part of a larger corporation like InterNLnet (part of Tele2).

that they are working on the adoption of Internet security standards, but in practice do nothing, as indicated by an interviewee (Interview BIT). Another respondent indicated that there is a public interest in putting this topic on the agenda. 'The pressure (for adopting DNSSEC) must come from somewhere.' (Interview InterNLnet)

Other stakeholders like the SIDN indicate that the Wet GDI creates a sense of urgency (Interview SIDN). The possibility of introducing a standard by AMvB will considerably shorten the introduction time, because there is no need to consult the parliament. There are also drawbacks, according to some interviewees. For instance, not all techniques are mature enough to become compulsory (for instance SPF, caused by trouble with the 'from' field (Interview BIT)). Also, an accurate description of the functional working area is needed. Currently, there is discussion for instance whether the internal network should be supporting DNSSEC, or should printers support DNSSEC. The current description is under review, (Forum Standaardisatie, 2017c), goal is to provide a provision that is simple and to be used in buying processes, as well as technically correct.

4.3.2 Access providers

A major limitation of the Wet GDI is, that it focusses only on implementing Internet security standards on the (semi-) public sector, where the adoption level of DNSSEC is already high. For adoption of DNSSEC by access providers there is much less attention. The two largest access providers (KPN and Ziggo, 80 – 85% market share) both do not support DNSSEC. As demonstrated in chapter 3, this part is largely overlooked in the comply-or-explain policy.

4.4 Current policy instruments

The department of Internal Affairs is primarily responsible for the regime set by the Wet GDI (in cooperation with the department of EZ), while the *Telecomwet* is designed by the department of Economic Affairs. Their visions on the role of the government differ. The department of Internal Affairs holds on to a clear role and on intervention by the government (Ministerie van Binnenlandse Zaken, 2015). In the opinion of the section Telecom the role of the department is more modest. Since Telecom is a dynamic and innovative market, government intervention should be kept minimal. This principle is reflected in the *Telecomwet*. Section Telecom is in general not in favour of imposing regulation on ISPs. (Interview Telecom EZ)

For the section Telecom, there are two criteria that legitimate government intervention. First, there should be an interest for society. This can be a public good. Second, the market must not be able to solve it, due to market failures. These market failures can refer to public goods and services, abuse of market power, failures like information asymmetry and high transaction costs, and (positive of negative) externalities. [58] As demonstrated earlier, both elements are present in this case.

According to the Telecom department there is a public interest in a secure .nl ccTLD, and that Internet security standards are supported. Basically, this has to do with trust. Cyber security infringements can cause consumers to shy away from web based services. Trust is important for innovation, that is stimulated by the department. The department deploys several initiatives (including the support of

[58] These principles are listed in *Aanpak ordeningsvraagstukken voor de elektronische communicatiemarkt* (Directie Telecom 2007, not published).

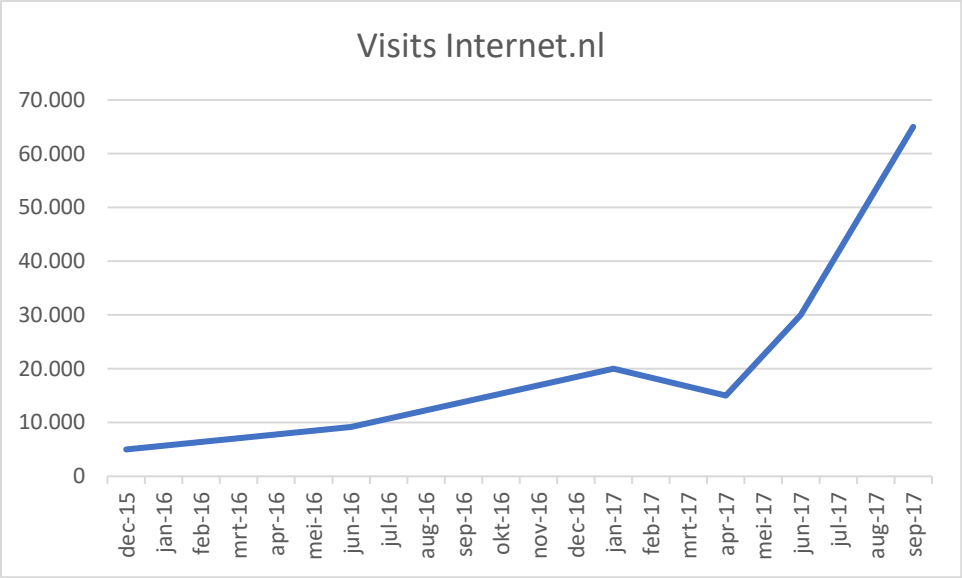
Internet security standards), that support this innovation. Part of the interest in the .nl ccTLD is the support of Internet security standards. (Interview Telecom EZ).

According to section Telecom the continuity and stability of the .nl ccTLD is of public interest. Therefore, in 2015 an agreement between the SIDN and the department of EZ was signed to make sure this interest is secured. This agreement entails that SIDN will continue to be in the Netherlands. This to make sure that all stakeholders are engaged in decision making about the .nl domain within the Dutch jurisdiction. Another provision states that in case of bankruptcy of SIDN, the department of Economic Affairs will provide necessary help. The self-regulating regime will be preserved, SIDN remains autonomous. (Rijksoverheid.nl, 2015)

There are several ways market failures can be corrected by regulation, as discussed in the first chapter. Telecom is more in favour of less intrusive initiatives such as public private partnership to put security on the agenda of ISPs. An example of this policy is the Abuse Information Exchange. This is a network initiative in which employees of ISPs can participate to correct information asymmetry, supported by the department of Economic Affairs. A tool has been developed, that can monitor malicious traffic. Goal is to analyse bot-net infections and correlate this with other sources at one point. This to inform end-users about the abuse of their computers by for instance botnets (an end-user is usually unaware of this) (Interview Telecom EZ).This can be regarded as an initiative by ISPs to take more responsibility to improve security within the network.

Failures like information asymmetry can be 'fixed' by offering better information. In cooperation with many partners as Forum Standaardisatie, ISPconnect, SIDN and others a tool has been developed (Interview Forum Standaardisatie) . With the tool Internet.nl, it is possible to see what standards are used for a certain domain name. This goes for DNSSEC (both signing and validation), but also for other standards such as SPF, DKIM, and DMARC. The tool also comprises details like correct implementation of a protocol. (Interview Forum Standaardisatie)

The number of visitors to Internet.nl rose gradually over the last two years, according to Forum for Standaardisatie. The number of tests has risen from approximately 5 k in December 2015 to 65 k in September 2017. Especially after the renewal of the website in July 2017 the number of visitors rose quite fast. Numbers of visitors do not say everything, but are an indicator for attention. In combination with the growing number of DNSSEC signed domain names, it can be concluded that the attention (and correlated signing) for Internet security standards is rising. So it is likely that Internet.nl is effective in fighting information asymmetry on this point.



Graphic 2. Number of visitors Internet.nl December 2015 – September 2017 (Figures Forum Standaardisatie)

4.5 Analysis and policy options

As discussed in the first chapter there are essentially three options available for the policy maker to increase the adoption of DNSSEC. These are introducing regulation, increasing public awareness, and introducing a financial incentive to adopt standards.

- *Introduce or adjust regulation*

An option for a policy maker is regulation by law. In this case, the *Telecomwet* regulates ISPs. Article 11.3, second section states that ISPs should adopt an appropriate security level to protect their customers against data-leakage and other cyber security risks. Since this provision is rather vague, it is very difficult to address liabilities. It is not clear what needs to be done to provide an appropriate security level.

A possibility for policy makers is to include a more explicit responsibility for ISPs in this provision. This could be done *ex ante*, by imposing standards. A requirement could be an appropriate security policy, including a comply-or-explain provision regarding Internet security standards. In this case, there is an incentive for ISPs to adopt security standards. Advantage of this approach is, that there is room to deviate from adopting standards in case there are good reasons to do so. It could include a compensation of costs, for instance for access providers since there is no business case to invest in these measures.

Another way is addressing responsibilities in the case of a security incident. This can be considered *ex post* regulation. There already exists a duty for ISPs to provide continuous telecom services. If availability is compromised, end-users can notify Agentschap Telecom. This also goes for leakage of personal information. It is possible to extent the duty to notify (*meldplicht)* in the *Telecomwet* about this. In the case of a security incident, an ISP has to prove that necessary mitigating measures have been taken. It could also be done in the *Wet gegevensverwerking en meldplicht cybersecurity* (Wgmc), that includes a duty to notify. The Wgmc is currently applicable only for large telecom operators (> 1 million customers). Due to the high threshold, this will only affect a limited number of companies (that are part of the vital infrastructure). (Ministerie van Justitie en Veiligheid, 2017)

There is also other legislation that is relevant. Cabinet Rutte II introduced in the government statement a right to do digital business for all citizens and entrepreneurs ("Regeerakkoord 'Bruggen slaan' | Rapport | Rijksoverheid.nl," 2012; 10). The Wet GDI is also part of this, as explained before. But also, other changes are needed to make sure this right is warranted. In the current situation a (semi-) public institution has to allow a citizen or entrepreneur to turn in a request in a digital mail.

To make sure that citizens and entrepreneurs can send a request by e-mail, a change of the *Algemene Bestuurswet* (ABW) is in preparation. A section 2.3 is added, in which a right to do digital business is included. This section entails conditions that secure electronic traffic between (semi-) public institutions and citizens and entrepreneurs. Article 2: 14 3th provision states that confidentiality and security of the messages must be warranted, given the nature and content of the message and the intended goal. As examples for safe e-mail traffic the Berichtenbox voor bedrijven and Mijn Overheid is noted, but this could also be done by using e-mail that is compliant with Internet security standards (such as DNSSEC). (Overheid.nl, 2016; 1)

Most discussed legal options are rather problematic. The introduction of a (legal) obligation for Internet security standards is rather intrusive, even if there is room to deviate. This also makes enforcement more complex. As shown earlier there are many stakeholders in the DNSSEC ecosystem, that have different roles and incentives to (not) adopt DNSSEC. These different stakeholders should be properly addressed in line with their responsibilities. Government intervention should be well designed and targeted.

Although cyber security has strong public good characteristics, the government is not in a good position to 'command and control'. Partly due to enforcement issues, only serious cyber security incidents can be addressed in legislation (duty to notify, Wmcg). Internet services are provided by ISPs, that are predominantly privately owned. ISPs are in a much better position to invest in cyber security, but especially for access providers there is no business case to legitimate such an investment. This implies that self-regulation is not an appropriate strategy. It must be recognised that ISPs cannot provide security on their own. The most appropriate strategy therefore to improve cyber security in the ISP sector is co-regulation.

- *Increase public awareness*

As indicated market failures like information asymmetry play a role in adopting DNSSEC. For end-users and registrants is difficult to see if DNSSEC is offered, against what price. Currently it is quite hard to compare several registrars. There are two examples of fighting market failures by correcting information asymmetry. By addressing cyber security issues to individual users, awareness rises, and more action can be expected. Internet.nl makes it possible to monitor what Internet security standards are used for a certain domain. As figures and reaction of interviewees indicate, this is a useful provision. A more transparent market increases choice, and reduces the constraint. (Lessig 2006; 123)

This approach can be extended by using approval marks. Individual icons like browser extensions for DNSSEC can be confusing (there are already a lot). An approval mark could be a solution for this. An option could be to determine a minimum set of requirements for a website to be approved. If approved, this can be shown by a sign to the end-user. This approach can be completed with educational measures, like a campaign.

A comparable measure has been taken quite recently by the department of Economic Affairs. In 2018 a Digital Trust Centre (DTC) will start to support small- and medium sized companies (SME) to fight cybercrime. The DTC will offer entrepreneurs information about digital threats and mitigating measures. As some interviewees indicate, it is difficult for SMEs to list topics themselves and implement appropriate measures (Interview Donner). An organisation as the DTC can be helpful to provide the required knowledge. (Rijksoverheid.nl, 2016b)

- *Introduce or extend financial incentives*

Large access providers are confronted with huge cost (several hundreds of thousands) to adopt DNSSEC. An option could be to contribute to costs that access providers have to make to adopt DNSSEC. The department of EZ has a huge variety of instruments that can shape this policy. Essentially large access providers have to invest, so policy instruments should support this. This makes instruments like subordinated credit and (financial) guarantees less suited. For instance investment incentives are more appropriate, such as tax cuts. Tax cuts based on the *Wet bevordering speur- en ontwikkelingswerk* allow ISPs to substract costs of working hours by employees from profit[59]. As indicated by interviewees, these costs are a main part of the total investment to adopt DNSSEC. In this way, instruments can be 'targeted' designed.

This approach could be combined with 'best practices'. A 'best practice' approach might be helpful to explore difficulties experienced by access providers. This can help to develop tools or open software solutions, that proved to be helpful for hosting providers. As a start, the offering of platform facilities for access providers might be useful. A proof of concept can be developed and implemented in one organisation. Step-by-step adoption showed successfull in other cases. (Moore, 2006; 4-5)

4.6 Conclusion

ISPs conduct a wide array of activities, that can be categorized in hosting and access. The adoption of DNSSEC by hosting providers (including registrars) has been (partially) successful, also because of the SIDN 'family and friends' program. On average about 49% of all domains are DNSSEC signed. Offering a DNSSEC signed domain name fits in a proposition in the more quality oriented high-market. Effects of unsecured domain names are not borne by these ISPs, but by registrants and end-users. This can be considered a *negative externality*.

For ISPs that provide validation services the business case is worse. Due to bogus domain names websites may become unreachable. Although most of this problem has been solved, DNSSEC is still perceived as risky and complex. On top of that, for large ISPs that provide access services the investment to adopt DNSSEC is considerable, and these ISPs do not benefit from it. So, it is no surprise the largest access providers KPN and Ziggo do not support DNSSEC.

These differences are clearly reflected in adoption levels (49% signed domain names, against 22% validation). As explained in the (semi-) public chapter risk appetite is an important factor in cyber security investments. These risks are generally lower for ISPs than for the (semi-) public sector. Partly because of this, checks and balances in the (semi-)public sector are absent here. In some cases, there

[59] For WBSO conditions see https://www.rvo.nl/subsidies-regelingen/wbso.

are additional costs for a hosting ISP to adjust (open source) software to be able to use it for their own networks. These factors all together explain why only 22% of the ISPs use DNSSEC for their own domain name.

The department of Economic Affairs is responsible for the regulation of the Telecom sector. Central paradigm is that a government should interfere as minimal as possible, to prevent disturbance of the market. Market failures or system failures are a legitimate ground for government intervention. These market failures can refer to public goods and services, abuse of market power, failures like information asymmetry and high transaction costs, and (positive of negative) externalities.

There are several ways market failures can be corrected by government intervention. As Friedman showed government intervention can oscillate between a very light regime like stimulation and more intrusive measures like a law. Legal options are including a comply-or-explain policy in the Telecom wet, the extension of the duty to notify (meldplicht), and the ABW regarding the right to do (safe) digital business. Examples of a lighter regime are Abuse Information Exchange and Internet.nl. The latter is an effective instrument to fight *information asymmetry*, given the rising number of visitors.

Cyber security has strong public goods characteristics, but the government is not in a good position to 'command and control'. Because of this, co-regulation between ISPs and public sector is the most effective strategy. Possible options that can be explored to increase for instance DNSSEC validation are co-financing necessary investments. Best practises can be effective to explore adoptable solution as a proof of concept in one company, that can be distributed to others.

Essential findings and discussion

Central question in this research is how the variance in adoption levels of DNSSEC signed domain names in the sector (semi-) public institutions and ISPs can be explained. To answer this question an exploratory case study is conducted, that include actors that provide the solution. Also, the different regulatory regimes of (semi-) public institutions and the ISP sector are taken into account. This includes some of the main pros and cons of expected regulation (Wet GDI).

There are several elements part of the question whether DNSSEC will be further adopted. First, there is no consensus about the added value of DNSSEC. There are certain advantages connected to the use of DNSSEC, especially concerning safe e-mail. A small group of frontrunners advocate DNSSEC, and as showed in best practices implementation is possible against acceptable costs. Problems with accessibility in the early stage of adoption have largely been solved. This is shown by ISPs like ASP4all and BIT, who have successfully adopted DNSSEC both on the hosting and the validation side.

On the other hand, there is a group much more sceptical towards the DNSSEC solution. According to this group, advantages of DNSSEC remain theoretical, since there are few incidents known related to the DNS. Phishing is still the most used method to spread malware, but it is not necessary to abuse the DNS for this. End-users can be deceived in many other ways than by manipulating the DNS. If a computer is infected, the client is also compromised and DNSSEC does not offer any protection against this.

A second element in the discussion are drawbacks of the DNSSEC solution. Critics of DNSSEC point towards accessibility problems caused by DNSSEC. Especially shortly after introduction accessibility of websites with bogus domain names caused serious problems. Although this problem has diminished, DNSSEC is still perceived as a complex solution that might endanger availability of services. In the case of financial services, this argument is being used not to adopt DNSSEC.

A third element is the business case for registrars and hosting providers. Due to the 'family-and-friends' program and other help signing of domain names is relatively high (on average 49%). Still a limited number of registrars offer DNSSEC and usually charge (much) more for a safe domain name. For a registrant it is not very attractive to invest in a more secure domain name. It is also possible that registrants do not consider DNSSEC necessary, given the nature of their business.

A fourth factor relevant for adoption on the hosting site are outsourcing of ICT and privately-owned DNS servers. Especially large firms outsource their ICT infrastructure to (Chinese) companies like Huawei. Since the worldwide adoption of DNSSEC is very limited, it is not very attractive from a business point of view to adopt DNSSEC. For companies that run their own DNS servers it is relatively more difficult to adopt DNSSEC. In many cases, knowledge how to do this is missing.

A fifth part relevant for (further) adoption is the business case for access providers. Although the problem of bogus domain names is largely solved, there is little reason for access providers to invest in the adoption of DNSSEC. Access providers can only lose by adopting DNSSEC. The low validation rate (22%) of access providers is also a reason for other stakeholders not to invest in adoption of DNSSEC. Thus, a 'chicken-and-egg' situation exists.

These factors together illustrate factors that hamper further adoption of DNSSEC. Without intervention by policymakers, it is not likely that adoption levels will increase. In the (semi-) public sector, the adoption of Internet security standards is secured by architects, buying department, DPC and audits. The comply-or-explain regime demands security standards to be required in the case of the purchase of ICT exceeding € 50 k. Although not watertight, these mechanisms explain all together the high adoption degree (59%) of DNSSEC signed domain names in the (semi-)public sector. The effectivity of this high adoption rate remains low, given the limited number of access providers that validate DNSSEC.

In the ISP sector, a minority provides a signed domain name. About 22% of these companies have adopted DNSSEC for their domain names. Partly due to lower perceived risks, checks and balances for DNSSEC adoption are absent here. Some (hosting) providers do offer DNSSEC for their customers, but do not use DNSSEC for their own domain names. This because of additional costs connected to securing their own domain names. These factors all together provide an explanation why the adoption in this sector is much lower than in (semi-) public sector.

Question is how worrisome this adoption level is. A central element in the approach should be a risk analysis. This analysis legitimises investments in cyber security. If a risk analysis points out that risks are limited or acceptable, it makes sense not to invest in a signed domain. It is rational to accept some degree of insecurity. In other cases, lack of adoption can be problematic. For instance, if sensitive (personal health or financial) information is exchanged. Main issue in the question is the development of the number of DNS related incidents, that can be prevented with DNSSEC. It is difficult to predict how this will develop.

The adoption of DNSSEC confronts us with a dilemma. Regulation by the government is very intrusive, and it is hard to target all actors. A public debate about how much security is enough is very difficult. Members of the parliament repeatedly ask questions about the adoption of internet security standards[60]. To exclude all risks the debate about adoption becomes absolute and leaves no room for deviation, even if there are good reasons to do so. This is also the case in the Wet GDI, in which an obligation is created for (semi-) public institutions to adopt Internet security standards.

On the other hand, if the adoption of DNSSEC is left to the market little will happen. In some cases (low risks) this will not have much effect. In cases in which sensitive information such as health or financial services is exchanged this can be problematic. Due to market failures, it cannot be expected that access providers or to a lesser degree hosting providers adopt Internet security standards. This also goes for registrants. It is not rational to pay considerably more for a domain name, without profiting from advantages. Also, in some cases a signed domain is of limited value, so it makes no sense to spend extra for a signed domain name.

[60] See for instance a motion of Oosenbrug/Veldman about the adoption of security standards by municipalities ("Motie Oosenbrug/Veldman over meer toepassen van open standaarden door gemeenten - Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2016 - Parlementaire monitor," n.d.)

A point that remains is how to internalise externalities and correct information asymmetries in the cases with a high risk. Both government regulation and self-regulation have considerable drawbacks. Cyber security has strong public goods characteristics and is provided by private companies. This makes co-regulation the best option to increase the adoption of DNSSEC. Several public-private initiatives have been started, like Internet.nl and Abuse Information Exchange that seem quite promising. Most important is a risk oriented and a targeted approach. Costs and benefits should be aligned with the risk appetite, and all actors within the ecosystem included.

As indicated during the introduction, the economic aspects of cyber security is a relatively new field. This research presents some tentative conclusions, that can be explored in more detail. For instance, further research can be conducted regarding costs and benefits for ISPs to adopt Internet security standards on a larger scale. This could also include large access providers, that have not adopted DNSSEC. Another discussed aspect is the risk of missing Internet security standards like DNSSEC. In many cases it is not clear what these risks exactly entail. As indicated, these aspects are important to justify cyber security investments, that should be based on a balanced outcome of costs and benefits.

References

Agentschap Telecom. (2017). Achtergronden van de Telecommunicatiewet | Agentschap Telecom. Retrieved September 2, 2017, from https://www.agentschaptelecom.nl/algemeen/wettelijk-kader/achtergronden-van-de-telecommunicatiewet

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488. http://doi.org/10.2307/1879431

Alert online. (2016). Cyber security awareness en gedrag 2016 | Alert Online. Retrieved September 1, 2017, from https://www.alertonline.nl/toolkit

Anderson, R. (2001). Why Information Security is Hard. *Annual Computer Security Applications Conference*. Retrieved from www.cl.cam.ac.uk/~rja14/#Econ

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., … Savage, S. (2013). Measuring the Cost of Cybercrime. In *The Economics of Information Security and Privacy* (pp. 265–300). Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-642-39498-0_12

Antić, Đ. (2014). DNSSEC deployment and challenges. *Proceedings of the 1st International Scientific Conference - Sinteza 2014*, 678–682. http://doi.org/10.15308/sinteza-2014-678-682

APNIC. (2017a). DNSSEC Measurement Maps. Retrieved October 19, 2017, from https://stats.labs.apnic.net/dnssec

APNIC. (2017b). DNSSEC Measurement Maps. Retrieved October 1, 2017, from https://stats.labs.apnic.net/dnssec

Arrow, K. J., & Debreu, G. (2007). Existence of an equilibrium for a competitive economy, *22*(3), 265–290.

Asghari, H., van Eeten, M., & Bauer, J. M. (2016). Economics of cybersecurity. *Handbook on the Economics of the Internet*, 262–287.

Atkins, D., & Austein, R. (2004). Threat Analysis of the Domain Name System (DNS). Retrieved from https://tools.ietf.org/html/rfc3833

Bauer, J. M., & van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10–11), 706–719. http://doi.org/10.1016/j.telpol.2009.09.001

Beck, U. (2006). Living in the world risk society. *Economy and Society*, *35*(3), 329–346. http://doi.org/10.1080/03085140600844902

Berg, B. L. (2009). *Qualitative research methods*. Pearson.

Bestuur, B. (2017). "Tandje erbij met e-mailbeveiliging overheid" - Binnenlands Bestuur. Retrieved August 23, 2017, from http://www.binnenlandsbestuur.nl/digitaal/nieuws/tandje-erbij-met-e-mailbeveiliging-overheid.9568109.lynkx

Black, J. (2002). Critical reflections on regulation. *Australian Journal of Legal Philosophy*, *27*(1), 1–36. Retrieved from http://www.lse.ac.uk/CARR

Böhme, R. (2010). Security metrics and security investment models. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6434 LNCS*, 10–24. http://doi.org/10.1007/978-3-642-16825-3_2

CBS. (2017). Drie kwart cybercrimedelicten niet gemeld. Retrieved November 5, 2017, from https://www.cbs.nl/nl-nl/nieuws/2017/39/drie-kwart-cybercrimedelicten-niet-gemeld

Centraal Planbureau. (2016). *Risicorapportage Cyberveiligheid Economie*. http://doi.org/10.1017/CBO9781107415324.004

Chung, T., Van Rijswijk-Deij, R., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A., & Wilson, C. (2017). Understanding the Role of Registrars in DNSSEC Deployment CCS CONCEPTS, *15*. http://doi.org/10.1145/3131365.3131373

Cowperthwaite, A., & Somayaji, A. (2010). The futility of DNSSec. *5th Annual Symposium on Information Assurance (ASIA10)*, 28. Retrieved from

http://www.albany.edu/iasymposium/proceedings/2010/ASIA10Proceedings.pdf#page=11
Deloitte. (2017). Dealing efficiently with cybercrime Cyber Value at Risk in The Netherlands 2017.
Deployment Guide: DNSSEC for Internet Service Providers (ISPs) | Deploy360 Programme. (2017). Retrieved August 9, 2017, from http://www.internetsociety.org/deploy360/resources/deployment-guide-dnssec-for-isps/
DNSSEC. (2017a). DNSSEC FAQ - DNSSEC.nl. Retrieved August 28, 2017, from https://www.dnssec.nl/wat-is-dnssec/faq.html#beschermt_niet
DNSSEC. (2017b). SIDN perst laatste DNSSEC-validatiefouten uit de .nl-zone - DNSSEC.nl. Retrieved November 19, 2017, from https://www.dnssec.nl/cases/sidn-perst-laatste-dnssec-validatiefouten-uit-de-nl-zone.html
DNSSEC. (2017c). Wat is DNSSEC?
DNSSEC.nl. (2017). DNSSEC FAQ - DNSSEC.nl. Retrieved October 17, 2017, from https://www.dnssec.nl/wat-is-dnssec/faq.html
Durumeric, Z., Adrian, D., Mirian, A., & Kasten, J. (2015). Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Mail Delivery Security. *Proceedings of the 2015 …*, 27–39. http://doi.org/10.1145/2815675.2815695
Eeten, M. van;, & Bauer, J. M. (2008). Economics of Malware. *Workshop on Economics of Information Security*, (June). http://doi.org/10.1787/241440230621
Emerce. (2017). Ziggo haalt KPN bijna in op vaste telefonie-markt - Emerce. Retrieved October 18, 2017, from https://www.emerce.nl/wire/ziggo-haalt-kpn-bijna-vaste-telefoniemarkt
Enisia. (2012). *The costs of DNSSEC deployment*.
Forum Standaardisatie. (2008). Toepassen van “pas toe of leg uit” | Forum Standaardisatie. Retrieved October 22, 2017, from https://www.forumstandaardisatie.nl/thema/toepassen-van-pas-toe-leg-uit
Forum Standaardisatie. (2017a). DNSSEC | Forum Standaardisatie. Retrieved September 3, 2017, from https://www.forumstandaardisatie.nl/standaard/dnssec
Forum Standaardisatie. (2017b). Pas-toe-of-leg-uit | Forum Standaardisatie. Retrieved October 22, 2017, from https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit
Forum Standaardisatie. (2017c). Verduidelijking functioneel toepassingsgebieden.
Friedlander, A., Mankin, A., & Maughan, W. D. (2005). DNSSEC and Hardening Security in the Internet Infrastructure: The Public Policy Questions, 1–12.
Friedman, A. (2011). Economic and Policy Frameworks for Cybersecurity Risks, 1–23. Retrieved from https://www.fbiic.gov/public/2011/jul/0721_cybersecurity_friedman.pdf
Ganan, C. et al. (2017). Beyond the pretty penny: the Economic Impac of Cybercrime. *Proceedings of New Security Paradigm Workshops, Islamorada Florida, USA, October 2017 (NSPW’ 17).* http://doi.org/10.1145/nnnnnnn.nnnnnnn
Google. (2017). IPv6 statistics. Retrieved August 18, 2017, from https://www.google.com/intl/nl/ipv6/statistics.html,
ICANN. (2017). Security Best Practices: DNSSEC Validation - ICANN. Retrieved October 23, 2017, from https://www.icann.org/news/blog/security-best-practices-dnssec-validation
IETF. (1999). Domain Name System Security Extensions. *Rfc 2535*, 1–48. http://doi.org/10.17487/RFC2065
IETF. (2005). DNS Security Introduction and Requirements. Retrieved from https://tools.ietf.org/html/rfc4033
Internetstandaarden, P. (2017). Intentieverklaring Veilige E-mail Coalitie Achtergrond van Veilige E-mail Coalitie.
ISO/IEC. (2014). ISO 27005:2011, *2011*.
Katz, M. L., & Shapiro, C. (1985). Network Externalities , Competition , and Com pati bility. *The Americaon Economic Review*, *75*(3), 424–440. http://doi.org/10.2307/1814809
Korpel, J., & Vreuls, J. (2016). Monitor Open standaardenbeleid - rapportage 2016, (december).
Lessig, L. (2006). *Code 2.0* (2e Edition). New York: Basic Books.

Lodge and Wegrich. (2012). *Managing regulation. Regulatory analysis, politics and policy*. Palgrave Macmilan.
McCarthy, K. (2016). Is DNSSEC causing more problems than it solves? • The Register. Retrieved August 28, 2017, from https://www.theregister.co.uk/2016/02/23/dnssec_more_problem_than_solution/
Ministerie van Binnenlandse Zaken. (2015). Kamerbrief over uitgangspunten wetgeving Generieke Digitale Infrastructuur | Kamerstuk | Rijksoverheid.nl. Retrieved August 27, 2017, from https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/04/kamerbrief-over-uitgangspunten-wetgeving-generieke-digitale-infrastructuur
Ministerie van Binnenlandse Zaken. WET GDI Memorie van Toelichting (2017).
Ministerie van Binnenlandse Zaken. (2017b). Wetsontwerp generieke digitale infrastructuur (GDI) | Publicatie | Rijksoverheid.nl. Retrieved October 22, 2017, from https://www.rijksoverheid.nl/documenten/publicaties/2017/08/30/wetsontwerp-generieke-digitale-infrastructuur-gdi
Ministerie van Economische Zaken. (2008). Besluit van de Staatssecretaris van Economische Zaken van 8 november 2008, nr. WJZ/8157380, tot vaststelling Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten. Retrieved from https://zoek.officielebekendmakingen.nl/stcrt-2008-837.html
Ministerie van Economische Zaken. (2017a). Kamerbrief over voortgang open standaarden 2016 | Kamerstuk | Rijksoverheid.nl. Retrieved June 30, 2017, from https://www.rijksoverheid.nl/documenten/kamerstukken/2017/05/09/kamerbrief-over-voortgang-open-standaarden-2016
Ministerie van Economische Zaken. (2017b). wetten.nl - Regeling - Telecommunicatiewet - BWBR0009950. Retrieved October 19, 2017, from http://wetten.overheid.nl/BWBR0009950/2017-07-01
Ministerie van Financien. (2017). Home — Rijksbegrotingsvoorschriften 2018. Retrieved October 30, 2017, from https://www.rbv.minfin.nl/2018
Ministerie van Justitie en Veiligheid. (2017). Besluit van 4 december 2017 tot aanwijzing van aanbieders, producten en diensten ten aanzien waarvan een plicht geldt om ernstige ICT-incidenten te melden (Besluit meldplicht cybersecurity). Retrieved January 2, 2018, from https://zoek.officielebekendmakingen.nl/stb-2017-476.html
Moore, R. A. T. (2006). The Economics of Information Security. *Science*, *314*(5799), 610–613. Retrieved from http://www.jstor.org/stable/20031627
Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. *Workshop on Deterring Cyberattacks: Informing Strategis and DEveloping Options for US Policy*, 1–401. http://doi.org/10.17226/12997
Moore, T. (2017). *Market failures*. Retrieved from ftp://delftxdownloads.tudelft.nl/EconSec101x-EconomicsCybersecurity/Week 4/EconSec101x-4a-transcript.pdf
Motie Oosenbrug/Veldman over meer toepassen van open standaarden door gemeenten - Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2016 - Parlementaire monitor. (n.d.). Retrieved November 25, 2017, from https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vjz5c8wj2hzv
Nationaal Cyber Security Centrum. (2016). Cybersecuritybeeld Nederland CSBN 2016.
National Cyber Security Centre. (2015). Cyber Security Assessment Netherlands 2015, 1–84. Retrieved from https://english.nctv.nl/.../25760-csan-5-v3.2-web-uk_tcm92-611157.pdf
Nederlandse Betaalvereniging. (2016). Jaarverslag 2016. Retrieved September 24, 2017, from https://www.betaalvereniging.nl/wp-content/uploads/Jaarverslag-Betaalvereniging-2016.pdf
Nederlandse overheidswebsites niet goed beveiligheid. (2017). *NRC Handelsblad*. Retrieved from https://www.nrc.nl/nieuws/2016/12/01/nederlandse-overheidswebsites-niet-goed-beveiligd-a1534443,
NOREA. (2016). NOREA - de beroepsorganisatie van IT-Auditors. Retrieved October 22, 2017, from

https://www.norea.nl/nieuws/2439/aandachtspunten-digid-assessments
Overheid.nl. (2016a). Overheid.nl | Consultatie Wet modernisering elektronisch bestuurlijk verkeer. Retrieved December 1, 2017, from https://www.internetconsultatie.nl/wet_modernisering_elektronisch_bestuurlijk_verkeer/details
Overheid.nl. (2016b). wetten.nl - Regeling - Kaderbesluit nationale EZ-subsidies - BWBR0024796. Retrieved December 3, 2017, from http://wetten.overheid.nl/BWBR0024796/2016-07-01#Hoofdstuk10
Ozment, A., & Schechter, S. E. (2006). Bootstrapping the Adoption of Internet Security Protocols, (WEIS06), 1–19. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.60.9876%5Cnhttp://research.microsoft.com/pubs/79178/weis2006.pdf%5Cnhttp://research.microsoft.com/apps/pubs/default.aspx?id=79178
Pham. (2016). The Great DNS Vulnerability of 2008 by Dan Kaminsky | Duo Security. Retrieved October 19, 2017, from https://duo.com/blog/the-great-dns-vulnerability-of-2008-by-dan-kaminsky
Poel, M. (2017). Evaluatie van het ICT-beleid van het Ministerie van Economische Zaken , Directie Regeldruk en ICT-beleid.
Post, D. G., & Kehl, D. (2014). Controlling The Cost of Internet Connectivity Infrastructure, (April).
Punter, L. M., Verhoosel, J. P. C., Folmer, E. J. A., & Luttighuis, P. H. W. M. O. (2010). Sturen op Open Standaarden : een handreiking voor overheidsorganisaties. Forum Standaardisatie. Retrieved from https://research.utwente.nl/en/publications/sturen-op-open-standaarden-een-handreiking-voor-overheidsorganisa
Regeerakkoord “Bruggen slaan” | Rapport | Rijksoverheid.nl. (2012). Retrieved December 1, 2017, from https://www.rijksoverheid.nl/documenten/rapporten/2012/10/29/regeerakkoord
Rijksoverheid.nl. (2011). Bestuursakkoord 2011 - 2015 | Convenant | Rijksoverheid.nl. Retrieved October 22, 2017, from https://www.rijksoverheid.nl/documenten/convenanten/2011/04/21/bestuursakkoord-2011-2015
Rijksoverheid.nl. (2015). Domeinnamen voor websites | ICT | Rijksoverheid.nl. Retrieved October 26, 2017, from https://www.rijksoverheid.nl/onderwerpen/ict/domeinnamen
Rijksoverheid.nl. (2016a). Beantwoording Kamervragen over beveiliging gemeentesites | Kamerstuk | Rijksoverheid.nl. Retrieved August 30, 2017, from https://www.rijksoverheid.nl/documenten/kamerstukken/2016/06/01/beantwoording-kamervragen-over-beveiliging-gemeentesites
Rijksoverheid.nl. (2016b). Digital Trust Centre geeft ondernemers advies over cybersecurity | Nieuwsbericht | Rijksoverheid.nl. Retrieved October 19, 2017, from https://www.rijksoverheid.nl/actueel/nieuws/2017/09/23/digital-trust-centre-geeft-ondernemers-advies-over-cybersecurity
Rijswijk, R. van. (2017). *Improving DNS Security A Measurement-Based Approach*. http://doi.org/10.3990/1.9789036543293 https://doi.org/10.3990/1.97890365432
Rogers, E. (2014). Diffusion of Innovation , 5 th ed ., Everett M . How does new innovation spread out ?, (1995), 0–2.
Schneier, B. (2007). A Security Market for Lemons - Schneier on Security. Retrieved October 24, 2017, from https://www.schneier.com/blog/archives/2007/04/a_security_mark.html
Schneier, B. (2007). Essays: Information Security and Externalities - Schneier on Security. Retrieved November 9, 2017, from https://www.schneier.com/essays/archives/2007/01/information_security_1.html
SIDN. (2017a). .nl stats and data. Retrieved October 1, 2017, from https://stats.sidnlabs.nl/#/dnssec
SIDN. (2017b). DNSSEC. Retrieved April 30, 2017, from https://www.sidn.nl/a/veilig-internet/dnssec
SIDN. (2017c). DNSSEC. Retrieved August 28, 2017, from https://www.sidn.nl/a/veilig-internet/dnssec

SIDN. (2017d). DNSSEC-beveiliging Nederlandse domeinnamen onder de maat.
SIDN. (2017e). SIDN : Domeinnaammarkt groeide door in eerste halfjaar. Retrieved August 30, 2017, from https://www.sidn.nl/a/kennis/domeinnaammarkt-groeide-door-in-eerste-halfjaar
SIDN. (2017f). SIDN : Registrar Scorecard: een programma gericht op kwaliteit. Retrieved October 18, 2017, from https://www.sidn.nl/a/nl-domeinnaam/registrar-scorecard-een-programma-gericht-op-kwaliteit
SIDN. (2017g). SIDN : Statistieken registrars. Retrieved August 31, 2017, from https://www.sidn.nl/a/kennis/statistieken
SIDN. (2017h). SIDN : ValiBox: DNSSEC-validatie thuis. Retrieved October 18, 2017, from https://www.sidnlabs.nl/a/weblog/valibox-dnssec-validatie-thuis
SIDN.nl stats and data. (2017). Retrieved August 8, 2017, from https://stats.sidnlabs.nl/#/dnssec
Simon, H. A. (1952). a Behavioral Model of Rational Choice, *69*(1), 99–118.
Stiglitz, J. (2008). Principles of regulation. *Economic Theory*, 1–25.
Swanborn, P. (1996). *Case study's Wat, wanneer en hoe?* Boom onderwijs.
"Tandje erbij met e-mailbeveiliging overheid" - Binnenlands Bestuur. (2017). Retrieved August 16, 2017, from http://www.binnenlandsbestuur.nl/digitaal/nieuws/tandje-erbij-met-e-mailbeveiliging-overheid.9568109.lynkx
TechRepublic. (2009). 5 tips for choosing a registrar for sites you care about - TechRepublic. Retrieved September 1, 2017, from http://www.techrepublic.com/blog/it-security/5-tips-for-choosing-a-registrar-for-sites-you-care-about/
wetten.nl - Regeling - Beleidsregels informatieplicht voor aanbieders over internetveiligheid (artikel 11.3 tweede lid van de Telecommunicatiewet) - BWBR0033401. (2013). Retrieved August 25, 2017, from http://wetten.overheid.nl/BWBR0033401/2013-04-01
XR Magazine. (2017). 2017 State of Cybercrime Report. Retrieved September 29, 2017, from http://www.xr-magazine.nl/nieuws/2609/trends-ontwikkelingen/2017-state-cybercrime-report
York, D. (2012). Challenges and Opportunities In Deploying DNSSEC. *Securing and Trusting Internet Names (SATIN)*.
Zainal, Z. (2007). Case study as a research method.
Zittrain, J. L. (2014). *The Future of the Internet and How to Stop It*. http://doi.org/10.1086/261502

Interviews

- Logius, Juan Guillen Scholten PhD, solution architect. The Hague, August 15, 2017
  Member of the expert committee Forum Standaardisatie.
- SIDN, Michiel Henneke, marketing manager and Marco Davids, research engineer. Arnhem, September 8, 2017
- BIT, Wido Potters, manager customer care. Ede, September 15, 2017
- Forum voor Standaardisatie, Bart Knubben, projectmanager Internet standaarden. The Hague, September 18, 2017.
- DICTU, Henk Romein, architect. The Hague, September 24, 2017.
- Donner, Eelco Zuidervaart, MT-lid ICT. Rotterdam September 26, 2017.
- InterNLnet, Maarten van der Tol, manager InterNLnet. October 4, 2017 (by telephone)
- Ministerie van Algemene Zaken, Jan van Boheemen, webadvisor. The Hague October 6, 2017
- Ministerie van Economische Zaken, section Telecom, Thomas de Haan, policy advisor. The Hague October 9, 2017.
- SURFnet, Roland van Rijswijk PhD, Innovator Internet security, October 17, 2017 (by telephone). Member of the expert committee Forum Standaardisatie.

Appendix I - Questions for interviewees

The DNS is a complex ecosystem with multiple stakeholders. The stakeholders are categorised in several groups (see below). This according to the specific function of the group. Next to some more general questions I have formulated specific questions for each group. This in line with their function. Some questions are not relevant for all interviewees in a category. The questions will be directed to those responsible for cyber security policy as a senior employee, project manager or architect. This group is in general best informed, and prepare decisions made on higher levels.

Forum Standaardisatie has a more general role in encouraging the use of standards for Internet security as DNSSEC. This supported by the Department of Economic Affairs. To some degree this also goes for Stichting Internet Domeinnaam registratie (SIDN). SIDN has also a role in issuing subdomains and in operating DNS servers. Two members of the Expert group Internet Security Standaarden will be interviewed to validate the outcome of the literature regarding more technical aspects of DNSSEC. To some extent the interview will be unstructured to collect additional information. Subsequently several representatives of the group that provide DNS services will be interviewed. This also goes for stakeholders that use DNSSEC solutions. This by conducting semi-structured interviews, based on questions formulated below.

General: technical aspects of DNSSEC

Largely unstructured interview with the goal to validate conclusions from literature study regarding technical aspects of the DNSSEC solution. Also, to collect additional information about the working of DNSSEC.

- Two members of Expert group Internet Security Standaarden

Questions

1. How does the technical community value the DNSSEC solution?
2. How do you balance pros and cons of the DNSSEC solutions in a technical sense?
3. Are you familiar with security incidents caused by DNS attacks?

Actors DNSSEC

For the semi-structured interviews with stakeholders the following list of questions are used.

- Stichting Internet Domeinnaam registratie (SIDN)
- Registrars + hosting
- Access ISPs

Questions:

SIDN

1. SIDN has had an incentive program for registrars to provide DNSSEC solutions. Was this effective?
2. The adoption rate of DNSSEC is slowly increasing, what are possible explanations?
3. DNSSEC is on the 'comply or explain' list from Forum Standaardisatie. Is this effective?
4. What other ways do you see for the government to stimulate implementation?
5. What do you think of an obligation for DNSSEC as prepared in the Wet GDI?
6. Is this proportionate?
7. Do you think it is cost effective?

ISPs

8. Does your organization provide DNSSEC-solutions (domain names and resolvers)?
9. Why or why not?
10. What are the costs connected to implementation?
11. Is your organisation supported by SIDN to implement DNSSEC?
12. Was this useful?
13. If not implemented in what circumstances would you consider implementing DNSSEC?
14. Are end-users aware of the DNSSEC solution?

Stakeholders using DNSSEC

- (Semi-) public sector as a user of domain names (registrant)
- ISPs as a user of domain names
- Registrants in general

15. What standards does your organization use for security policy?
16. Does your organisation use DNSSEC?
17. Why of why not?
18. Who is responsible for the implementation of the policy (outsourced or not)
19. Is the list of Forum Standaardisatie considered?
20. Is the scope of the DNSSEC provision of Forum Standaardisatie clear?
21. Does the 'comply or explain list' by Forum Standaardisatie help implementing DNSSEC?
22. If not, why?
23. Is the 'comply or explain list' enforced, i.e. have you experienced sanctions for not complying?
24. How is the progress monitored within your organisation?
25. What could the government do to stimulate implementation?
26. Would a law be helpful?
27. If not, why not?
28. What recommendations do you have for current procedures ('comply or explain list')?

Policy makers

- Forum Standaardisatie
- Department Economic Affairs, Telecom department
- Dienst Publiek en Communicatie

Department of Economic Affairs and Internal Affairs are working on a law GDI that provides an obligation for DNSSEC.

29. What do you think of the proportionality of this measure?
30. Is 100% use of DNSSEC domains possible?
31. Is 100% DNSSEC signed domain names needed?
32. How long do you think it is going to take to implement this measure?
33. Who is going to pay for costs to implement DNSSEC?
34. Who is going to pay for audits?
35. Who is going to enforce the law?
36. Will this law effect the level playing field?
37. Telecom law provides duty of care for customer. Is this a useful provision in this case?

Appendix II - Interviewees and their role

Participant	Role	Who
Policy maker	- 'comply-or-explain' policy - Telecomwet - Wet GDI	- Department of Economic Affairs - Forum Standaardisatie - DPC
Registry	- Trust anchor - Zone operator	- SIDN
Registrar + hosting/ISP	- Issuing domain names - Signing domain names - Hosting nameservers	- InterNLnet - BIT - DPC
Validating/ISP	- Validating DNS queries	- KPN and Ziggo did not want to cooperate with the research
Registrant (semi-) public sector	- Consumer of domain names	- DPC - DICTU - Logius (DigiD)
Registrant ISPs	- Consumer of domain names	- BIT - InterNLnet
Registrant	- Consumer of domain names	- Donner
DNS experts	- Validating technical working DNSSEC conclusions	- Two members of the expert committee of Forum Standaardisatie.