enisa
European Network and Information Security Agency

THE COSTS OF **DNSSEC** DEPLOYMENT

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for enquiries on this study, please use the following details:
Technical Department, Security Tools and Architectures Section
Email: sta@enisa.europa.eu
Web: http://www.enisa.europa.eu/act/res/technologies/tech/dnssec/dnssec

This study has been prepared by the Security Tools and Architectures Section of ENISA in collaboration with Deloitte Enterprise Risk Services.

Acknowledgments

The authors would like to express their gratitude to all of the people and organisations that have participated in the various meetings, survey and interviews and without those contributions and dedications this report would not have been completed.

Our appreciation is also extended to the members of ENISA's Expert Group on DNS and CENTR (council of European national top level domain registries) who contributed throughout this activity.

Contents

1 Executive Summary

1 Executive Summary

The European Network and Information Security Agency (ENISA) is executing a Multiannual Thematic Program (MTP1) with the ultimate objective to collectively evaluate and improve the resiliency of public eCommunications[1] in the EU. As part of these program innovative technologies that had the potential to increase the resilience of such communications were investigated[2]. DNS Security Extensions (DNSSEC) has been identified as an important technology that could improve resilience, trustworthiness and quality of the internet's Domain Name System (DNS). It is complementary to other technologies like Secure Sockets Layer that secure the delivery of the content in increasing the security of online services.

Deploying a new technology requires investment in software, hardware and human resources. In the case of DNSSEC the cost of these investments is not well defined and this uncertainty can hinder its deployment. The Agency - in collaboration with a DNS Expert Group that assembled and Deloitte - were engaged in studying the costs and resource impact of DNSSEC deployments. The study was performed between June and September 2009.

The main observations and conclusion of this study are summarised in this executive summary:

Early adopters lead the pack

This study showed that - through the open knowledge sharing within the DNS community – organisations considering implementing DNSSEC can greatly benefit from the work performed by the pioneers and early adopters. This knowledge sharing is mainly focussed around sharing information and experiences. However, some DNS organisations chose to release some of their tooling and software to the general public by releasing it as open source software.

Organisation Types

Through analysis of the collected data, we noted that the cost of implementing DNSSEC is the lowest for pure registrars. Registries and (reverse) zone operators seem to have comparable costs with regards to their implementation projects.

In our analysis we identified two types of organisations implementing DNSSEC:

Big spenders;

Big savers;

Although their main business drivers for implementing DNSSEC are similar, big spenders and big savers are distinguished by their cost drivers and the maturity of their organisations with regards to IT processes.

Cost drivers

Based on the information obtained through the stocktaking we concluded that two important parameters exist in determining the cost drivers of a DNSSEC implementation project:

- Infrastructure cost: Big savers tend to reuse the overcapacity in their existing infrastructure for their DNSSEC implementation. Big spenders tend to use the DNSSEC implementation as an opportunity to upgrade their name server infrastructure.

[1] http://www.enisa.europa.eu/act/res
[2] http://www.enisa.europa.eu/act/it/library/deliverables/stock-tech-res
http://www.enisa.europa.eu/act/it/library/deliverables/res-feat

- Strategic positioning: Big spenders want to be in the frontline of the DNSSEC wave and choose to improve existing open source software through in-house development. Furthermore, big spenders also put more emphasis on the governance aspects of the DNSSEC implementation. At the other end of the spectrum are the big savers that mainly leverage on existing open source software and that limit customization and development efforts. Their strategy seems to be to implement DNSSEC in a lean way to ensure that their technology fits its purpose without considering the increased responsibility of being a Trust Anchor. The big spenders invest a significant amount of money in managing their increased responsibility. For example, the involvement of legal experts into the DNSSEC implementation project to ensure the responsibilities and possible legal implications of domain name signing.

Benefits & costs in the Value Chain

This section summarizes the analysis in simplified recommendations and food for thought for parties that did not yet adopt DNSSEC. It highlights the potential business benefits and an organisations motivation to implement DNSSEC as well as the anticipated capital and operational expenses for the different roles in the DNSSEC value chain.

Role	Business Benefits and Motivation	Anticipating Capital and Operational Expense
Registry	• Become a reliable Trust Anchor and boost market share and/or reputation of zones; • Lead by example and stimulate parties further down in the chain to adopt DNSSEC; • Earn recognition in the DNS community and share knowledge with TLD's and others.	• Being a trust anchor requires mature business processes, especially in key management;

Registry or zone operator		• Budgetary fork between 250.000€ and 1.250.000€ investment cost;
		• Investment cost strongly depends on current infrastructure utilization:
		  • If existing infrastructure is over dimensioned try to fit DNSSEC without new infrastructure;
		  • If no capacity is available use DNSSEC deployment
		  • for major infrastructure upgrade;
		• Investment cost also depends on strategic positioning towards DNSSEC: leaders pay the bill, followers can limit their investment;

Zone operator	• Provide assurance to end-user that domain name services are reliable and trustworthy; • Look forward to increasing adoption rate when revenue is an important driver. Deploying DNSSEC can be profitable; • Seek support from and collaboration with registries before and during DNSSEC deployment.	• Technical component of the investment – such as customisation and development – is approximately 20% of budgetary fork. Do not limit the deployment to this part only; • Financial cost might not outweigh the financial benefits. Prepare to write off the financial investment over 3 to 5 years, needed to gear up end-user equipment with DNSSEC.

Role	Business Benefits and Motivation	Anticipating Capital and Operational Expense
Registrar	• Use DNSSEC offering as a differentiator and competitive advantage versus other registrars.	• Budgetary quote of 10.000€ investment cost; • Investment cost is proportional with the complexity of the registrar's retail process. The cost does not depend on number of zones or size of organisation.

Recursive Resolver Operator	• Provide assurance to end-user that domain name services are reliable and trustworthy;
	• Use DNSSEC offering as a differentiator and competitive advantage versus other recursive resolver operators / Internet Service Providers
		• Budgetary fork between 15.000€ and 265.000€ investment cost;
		• Investment cost strongly depends on current infrastructure utilization:
		  • If existing infrastructure is over dimensioned try to fit DNSSEC without new infrastructure;
		  • If no capacity is available use DNSSEC deployment for major infrastructure upgrade;

Adoption

This study shows clearly that the technological readiness for DNSSEC in name servers (deployed name servers supporting the DNSSEC protocol) is much higher than the amount of actually signed zones. This should come as no surprise, since the supporting technical infrastructure should be in place before zones can be signed.

On the other hand, DNSSEC adoption by end users is still very low; this is mainly due to low awareness around DNSSEC and lack of signalling towards the end user. An end user who is running a client operating system which is not supporting DNSSEC can still rely on a recursive resolver operator (e.g. the users' ISP) to perform the required DNSSEC verifications. In such an environment, the recursive resolver operator would receive the potential errors related to DNSSEC and pass them on to the end user as a regular DNS error.

2 Background

2 Background

Resilience and security of communication networks and services that they support is an issue of critical importance to the EU economy and its citizens as it impacts day-to-day operation of businesses and affecting daily lives of EU citizens. In its reform proposals amending the current regulatory framework[3] (eCommunications Directive) the European Commission recognising the importance of resilience of communications networks and services proposed increased responsibilities for network operators through stronger obligations to ensure security and integrity and the mandatory requirement for breach notifications to National Regulatory Agencies (NRA) and consumers.

Resilience of public communications network is expected to play a major part in driving forward the growth of the EU economy. The ICT sector contributes 25% to the EU's GDP growth and 40% to its productivity growth[4]. In this light, it is of strategic importance to work towards securing European ICT infrastructures in support of EU development priorities. All efforts should be made in order to ensure that growth of the European industry will not be hindered by unreliable and unsecure network access to infrastructures. This is likely to happen if Europe does not put effort in the development and deployment of new, emerging technologies and architectures.

ENISA, the European Network Information Security Agency, recognised this need and launched a programme[5] with the ultimate objective to collectively evaluate and improve the resilience of public communications networks in Europe. In terms of technologies, the deployment of existing and emerging technologies as Internet Protocol version 6 (IPv6), Domain Name System Security Extensions (DNSSEC) and Multi Protocol Label Switching (MPLS) were investigated to assess their potential in providing increased network resilience. The results of this assessment, both in terms of security features[6] as well as how they are perceived by the operators of communication networks[7], indicate, among other things, the need to increase the security and availability of Domain Name System using a form of a Key Infrastructure. DNS Security Extensions has been identified as a technology that could improve DNS's resilience.

At the "Improving the resilience of DNS"[8] on January 28th 2009, in Athens, the possible actions that ENISA should take up were introduced and the formation of an experts group on DNSSEC was decided. One of the actions that were proposed by the experts group was to study the costs of deploying DNSSEC.

Deploying a new technology requires investment in software, hardware and human resources. A new technology such as DNSSEC might impose higher strains in the hardware and software in the implementation and maintenance phases of the deployment. New operational procedures have to be established and existing ones need to be updated. The staffs have to be trained and get accustomed with the new operational procedures.

Most of the domain names are following a registrant – registrar – registry model[9] for their administration. While for the DNS operation the zone operators and resolver operators are involved. The deployment of

[3] http://ec.europa.eu/information_society/policy/ecomm/library/proposals/index_en.htm
[4] "The Role of ICT in the Economic Growth and Productivity of Andalucia", JRC Scientific and Technical Report, EUR 22781EN – 2007, European Commission, DG JRC-IPTS, http://ftp.jrc.es/EURdoc/22781-ExeSumm.pdf
[5] http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_desig_ver_2008.pdf
[6] http://www.enisa.europa.eu/act/it/library/deliverables/res-feat
[7] http://www.enisa.europa.eu/act/it/library/deliverables/stock-tech-res
[8] http://www.enisa.europa.eu/act/res/workshops-1/2009/1st-dnssec-deployment-workshop/1st-workshop-on-dnssec-deployment
[9] IETF - Network Working Group Draft - Explanation of the registry/registrar concept http://tools.ietf.org/html/draft-faltstrom-registry-registrar-00

DNSSEC in the distinguished, different roles of the DNS administration and operation requires different changes in different resources of each role. The communication between the above mentioned roles may follow different protocols that may also differentiate between domains. Furthermore, several roles in the hierarchy might choose not to deploy DNSSEC, imposing additional costs to other roles.

Deloitte assisted ENISA in this effort by developing the methodology for the survey, conducting the survey and deliver a final report after consultation with relevant stakeholders.

This report presents the results of the study.

Reading instructions

The following guidelines should be taken into account when reading this document:

- In the published tables and graphs, data is always filtered on relevance;
- In order to provide the reader with a clear overview, subsets of data containing only the relevant information, have been used to create tables & graphs;
- The numbering of stakeholders (ID) and country location has been randomized in each table to ensure anonymity for participants. The ID is on purpose not consistent across multiple sections
- Quotes from stakeholders have been included throughout this report in the form of blue background tables;

3 Objectives & Scope

3 Objectives & Scope

3.1 Objectives

The objective of this study on DNSSEC deployment amongst different roles in the domain of DNS within the European Union and its member states was to:

- Study the costs (CAPEX/OPEX) of DNSSEC deployment
- Assess the required changes on resources of the different identified roles and operations in case of DNSSEC deployment
- Analyze the investments that deployment of DNSSEC would require through stocktaking and interviews

The study primarily focused on the costs of DNSSEC deployment and the changes required in order to deploy based on experience by the different roles that are targeted in the stocktaking and interview activities.

3.2 Scope

The scope of the survey was to study the costs of DNSSEC deployment through a targeted stocktaking and interviewing different roles in DNS administration and operation. The identified roles were registries, registrars, zone operators and recursive resolver operators.

The study was performed with the different identified roles within EU Member States and stakeholders from the USA. The minimum number of involved stakeholders in the survey was set to 20. The study was performed between June and September 2009.

4 Survey Respondents

4 Survey Respondents

The stocktaking as well as the interviews has been conducted between June and August of 2009. All participants were selected in a joint effort by ENISA, ENISA's expert group on DNS, CENTR (council of European national top level domain registries) and Deloitte. The respondents voluntarily participated in this study. The following organisations have participated.

Organisation	Country
Active24	CZ
Colt Telecom	DE
Forpsi	CZ
Frobbit	SE
Generalregistry	CZ
IIS	SE
IKS GMBH	DE
Interlan	SE
Loopia	SE
Neustar	US
NIC cz	CZ
NLNetlabs	NL
Nominet	UK
Microsoft	US
PIR (.org registry)/Afilias	US
RIPE	NL
SIDN	NL
Studio Barbero/Visiant Outscourcing	IT
SurfNET	NL
TeliaSonera	SE

Further information on the organisations that participated in the study are available in Appendix A.

All our stakeholders have been categorized as small, medium or large organization based on the total number of zones they serve at the moment. The following division guidelines have been used:

- Small organization: 0 to 99.999 zones
- Medium organization: 100.000 to 999.999 zones
- Large organization: as of 1.000.000 zones

The SecSpider monitoring project [10]from the UCLA University of Los Angeles shows that DNSSEC is not yet commonly used. However, the number of DNSSEC signed zones is growing every day. In order to obtain information that is realistic and relevant for the different roles within the domain name system hierarchy and to ensure that conclusions are not specific for particular countries, it was important to establish a survey population that had sufficient coverage on the different roles as well as within different countries.

The first selection criterion was to only consider candidates that had considered, implemented or abandoned a DNSSEC implementation. Given the objectives of this study and thereby the type of information to be gathered, only candidates matching this criterion could provide valuable input.

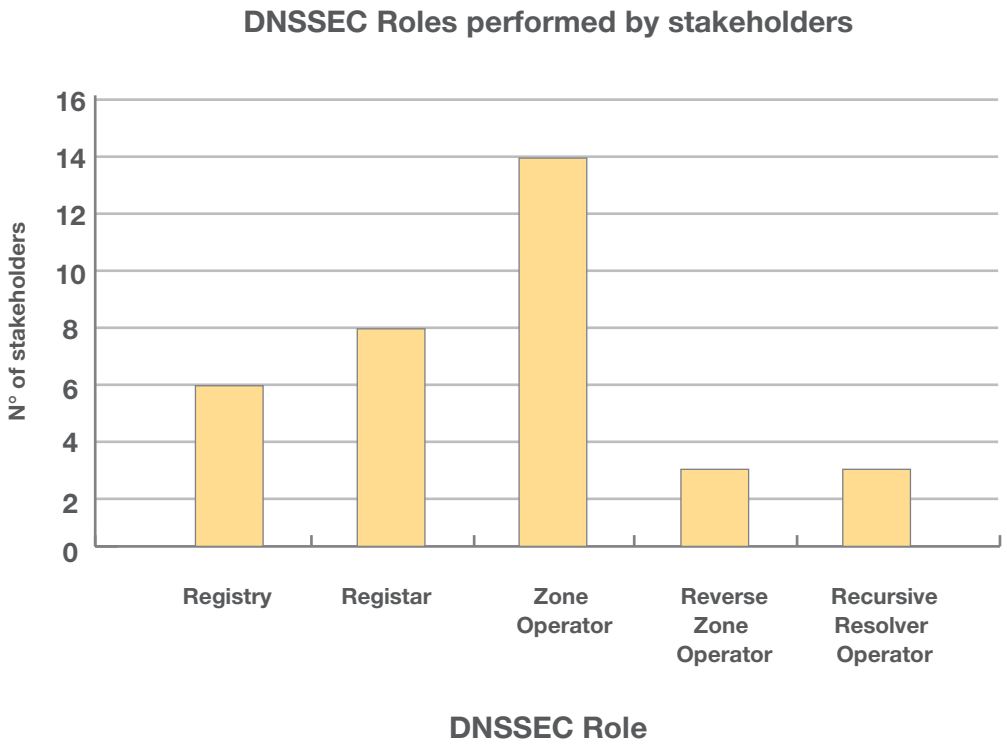
It should further be pointed out that participation in this study was voluntary and therefore, all information used in this study as well as the conclusions made on this information were based on answers and feedback obtained from parties matching our selection criteria that agreed upon participation in this study.

The study results are based on the information obtained through interviews and questionnaires completed by the participating organisations. A total of 33 roles have been identified. The participating organizations can be subdivided into following roles:

- 6 Registries
- 8 Registrars
- 14 Zone Operators
- 3 Reverse Zone Operators
- 3 Recursive resolver operators

[10] http://secspider.cs.ucla.edu/

It should be noted that an organization can have more than one role.



Following abbreviations will be used throughout this document to identify the role(s) of the participants:

Registry (RY): a registry is an organisation or commercial entity which:

- manages the registration of domain names within the top level domains for which it is responsible;
- controls the policies of domain name allocation;
- is responsible for the technical operations of its top-level domain;

Registrar (RAR): a registrar is an organisation or commercial entity which is accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) or by a national country top-level domain (cc-TLD) authority, to manage the reservation of Internet domain names in accordance with the guidelines of the designated domain name registries and offer such services to the public.

Zone Operator (ZO): a zone operator is an organisation which is responsible for the technical operation of dns zones and/or domain names. This typically involves operating the name server infrastructure:

- zone operators operate name servers which contain all dns records for a number of zones / domain names for which these servers are authoritative;
- reverse zone operators operate name servers which translate ip addresses into domain names (using the in-addr.arpa reverse name resolution hierarchy);

Recursive Resolver Operator (RRO): a recursive resolver operator operates name server infrastructure which is used by end users to resolve domain names to ip addresses. Internet service providers often have the role of recursive resolver operator.

5 Analysing Capital Expense

5 Analyzing Capital Expense

Capital expenditures (CAPEX) are expenditures to create future benefit and they are incurred when an organisation spends money to buy assets or to add to the value of existing assets.

In this chapter we provide an in-depth look into the DNSSEC-related capital expenditures of the organisations that participated in our survey.

5.1 Overall Investment Cost

Participants were asked to specify which investment costs were incurred or are planned for the deployment of DNSSEC in their particular environment. The correlation between investment costs and the role of the participant clearly highlights significant differences in cost structures between at one end registries and at the other end registrars and (reverse) zone operators. Based on the data obtained through the stocktaking we conclude that the DNSSEC implementation cost for registrars is negligible while the DNSSEC implementation cost of registries and zone operators are comparable.

Pure play registrars

Participants that only offer registrar services indicated that the investment cost is below 5.000€ for adopting DNSSEC into operations. By definition, registrars focus on reselling of domain names, as such they do not operate any DNS server. In this reselling process DNSSEC is only one simple attribute as part of the client's purchase. Including this attribute in the registrar's toolbox is the sole activity that a pure play registrar should undertake to adopt DNSSEC in its operational processes, which explains the relative low investment cost.

Table 1 – **Total CAPEX cost for pure play registries**

# ID	Role	Total CAPEX Cost
# 21	RAR	4.620€
# 18	RAR	0€

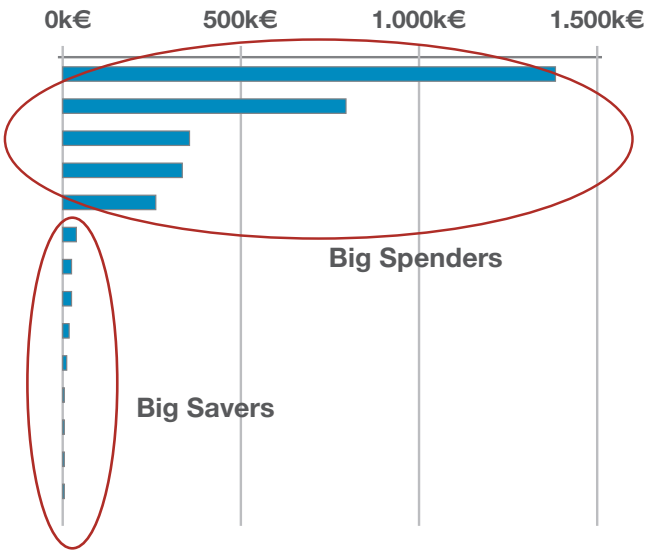
Registries and zone operators

Registries and zone operators both have to maintain operational DNS servers. An analysis of the capital expense for DNSSEC implementation in both categories revealed that the investment cost for registries is comparable with the investment cost for zone operators.

Comparing the participant's responses in this subset there is a clear distinction between two major categories: the "big savers" and the "big spenders". The big savers succeed in adopting DNSSEC with on average 27.000 € investment, while the big spenders invest on average 608.000 €.

Table 2 – **Total CAPEX cost for Registrars and Zone Operators**

# ID	Role	Total CAPEX Cost
# 17	RY; ZO	1.329.940€
# 18	RY; ZO	787.700€
# 11	ZO	335.590€
# 1	ZO; RRO	321.000€
# 12	RAR; ; ZO; RRO	266.240€
# 4	ZO	36.059€
# 2	RY; RAR; ZO	28.600€
# 20	ZO	26.023€
# 6	ZO	22.617€
# 19	RAR; ZO; RRO	17.000€
# 10	RAR; ZO	6.575€
# 5	ZO	5.100€
# 13	RAR; ZO	4.855€
# 4	RAR	4.620€



There is no clear correlation between investment cost and number of zones or number of daily queries. As such, the investment cost is not dictated by the size of an organization.

Table 3 – **No correlation between CAPEX and # of zones or # of queries**

# ID	Role	Total Zones	Total Daily queries	Total CAPEX Cost
# 2	RY; ZO	2	1.000.000.000.000	1.329.940€
# 3	RY; ZO	45	3.750.000.000	787.700€
# 11	ZO	20	648.000	335.590€
# 14	ZO; RRO	701	90.000.000	321.000€
# 17	RAR; ZO	80.000	238.291.200	266.240€
# 10	ZO	155	9.072.000.000	36.059€
# 5	ZO	520	80.000.000	22.617€
# 12	RAR; ZO	500.000	259.202.000	6.575€
# 1	ZO	400	510.000	5.100€
# 7	RAR; ZO	175.216	72.000.000	4.855€

Consequently, other parameters are at play. Based on participant's responses on capital expenditure this study reveals that the two most important cost drivers are:

- infrastructure cost;
- strategic positioning.

This section goes into detail for both parameters.

Infrastructure Cost

A first parameter that makes the difference is the infrastructure cost. The big savers indicate in their responses that the infrastructure investment was typically less than 10.000€, effectively meaning that DNSSEC is operational on the same infrastructure that was in place prior to deployment. The underlying cause might be that typical DNS infrastructures have relatively low utilization and overcapacity in CPU and storage. This overcapacity will now be used by DNSSEC.

Contrary, the big spenders indicate that there is a need for significant investments in new infrastructure components, ranging from 17% until 48% of the total investment cost. Apparently, organizations in this category consider it necessary to significantly upgrade their infrastructure when adopting DNSSEC.

Table 4 – **Big spenders invest % of CAPEX for infrastructure**

# ID	Role	Total CAPEX Cost	Infrastructure CAPEX Cost	% Infra in CAPEX
# 13	RY; ZO	1.329.940€	522.000€	39%
# 4	RY; ZO	787.700€	375.000€	48%
# 3	ZO; RRO	321.000€	56.000€	17%
# 16	RAR; ZO; RRO	266.240€	80.000€	30%

Strategic Positioning

"DNSSEC is new technology: testing and training are crucial elements of a successful deployment"

A second parameter that differentiates big savers from big spenders is their strategic position towards DNSSEC. Big spenders want to be in the frontline of the DNSSEC wave and choose to improve existing open source software through in-house development. Additionally, big spenders also put more emphasis on the governance aspects of the DNSSEC implementation. This strategy became visible in the survey when big spenders responded to questions regarding key management and formalised operational processes. At the other end of the spectrum are the big savers that mainly leverage on existing open source software and that limit customization and development efforts. Their strategy seems to be to implement DNSSEC in a lean way to ensure that their technology fits its purpose without considering the increased responsibility of being a Trust Anchor for particular zones.

Strong focus on technology can also be deduced from the headcount comparison between administrative and technical staff. This study is using the share of technical staff in the total employment of the respondents as an indicator for their strategic position. The table below gives the absolute figures for both the big spenders and the big savers.

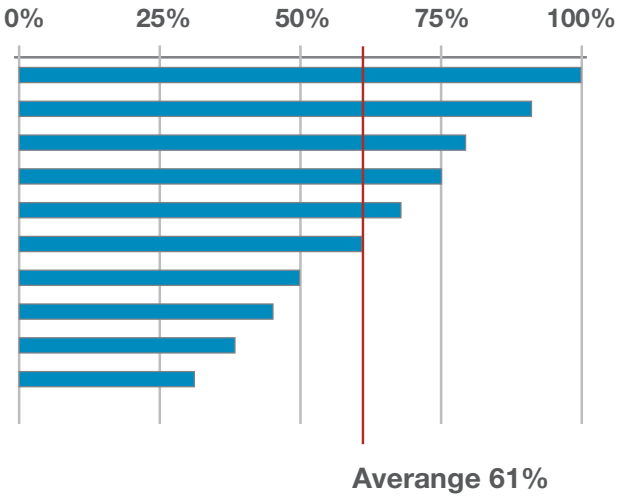
Table 5 – **Admin staff versus Tech staff for big spenders and big savers (absolute figures)**

# ID	Role	Total CAPEX Cost	Admin Staff	Tech Staff
# 8	RY; ZO	1.329.940€	400	600
# 21	ZO	335.590€	1	6
# 19	ZO; RRO	321.000€	9	61
# 2	RY	81.625€	98	33
# 11	RY	41.800€	11	11
# 6	ZO	36.059€	0	3
# 15	RY; RAR; ZO	28.600€	25	17

Comparing participants in the big saver category reveals that on average 61% of their staff is technically oriented.

Table 6 – **Admin staff versus Tech staff for big savers (relative figures)**

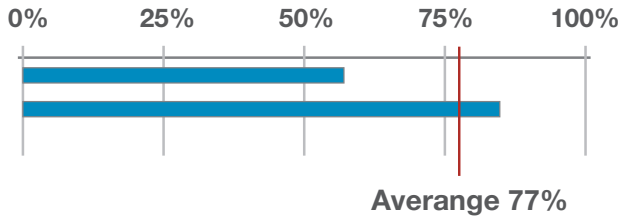
# ID	Role	% Technical staff
# 6	ZO	100%
# 20	ZO	90%
# 15	RAR; ZO; RRO	79%
# 14	RAR; ZO	75%
# 17	ZO	67%
# 2	RAR; ZO	61%
# 11	RY	50%
# 7	RAR	46%
# 10	RY; RAR; ZO	40%
# 1	ZO	33%
# 20	RY	25%



Contrary, big spenders reach an average of 77% of technical staff. Looking back at the absolute figures on staff employment there is no clear correlation between the size of the organisation and the percentage of technical staff.

Table 7 – **Admin staff versus Tech staff for big spenders (relative figures)**

# ID	Role	% Technical staff
# 7	RY; ZO	60%
# 20	ZO	85%
# 19	ZO; RRO	87%



As a conclusion, it seems fair to state that for now the overall investment cost of registries and zone operators is mainly defined by the infrastructure cost and the strategic positioning towards DNSSEC of one particular organisation.

5.2 Software cost

Almost none of the correspondents have bought a commercial-of-the-shelf (COTS) DNS product, so all software costs come from customization of open source solutions or in-house development. This in-house software development is a strong cost driver for some of the interviewed parties.

Based on the interpretation by the interviewees early adaptors were obliged to invest significantly in in-house development, which was definitely the case for organizations that adopted DNSSEC before 2008. This can largely be attributed to the fact that early adopters were considering DNSSEC partially as a study project and that they have made investments in identifying needs previously unanticipated by DNSSEC and extensions for DNSSEC as well as subsequent developments to fulfil these needs.

Late adopters - implementing DNSSEC after 2008 – have the ability to benefit from these developments by using the latest open source solutions. The cohesion in the DNS community and the open collaboration between different organizations allowed late adopters to benefit from the development of early adopters. Based on the figures of the survey, it appears to be the technology-oriented organizations that are able to reduce their software cost while the governance-oriented organizations still need in-house development to fit the open source solutions in mature operational processes. Nevertheless, the implementation effort has significantly dropped over the past few years and has now become predictable.

Open source software is very popular within all sizes of organizations. 83% of the stakeholders indicated that they use open source software for their DNSSEC deployment. The use of open source software is mostly combined with a small part of in-house developed software for interfaces towards the other parties in DNSSEC and for frontend solutions.

Exceptions on the above choose to outsource the operational aspects of running a registry or zone operator to a service provider who will perform the service on their behalf.

The table below gives an overview of the development cost compared to the total investment cost.

Table 8 – **% of CAPEX for Development**

# ID	Role	Total CAPEX Cost	Development Cost	% Dev in CAPEX
# 20	RY; ZO	1.329.940€	807.940€	61%
# 2	RY; ZO	787.700€	252.700€	32%
# 19	ZO	335.590€	335.590€	100%
# 6	ZO; RRO	321.000€	185.000€	58%
# 18	RAR; ZO; RRO	266.240€	76.240€	29%
# 1	RY	81.625€	81.625€	100%
# 7	RY	41.800€	39.800€	95%
# 5	ZO	36.059€	33.559€	93%

# ID	Role	Total CAPEX Cost	Development Cost	% Dev in CAPEX
# 4	ZO	26.023€	15.333€	59%
# 9	ZO	22.617€	21.117€	93%
# 3	RAR; ZO; RRO	17.000€	16.000€	94%
# 17	RAR; ZO	6.575€	5.675€	86%
# 11	ZO	5.100€	3.100€	61%
# 23	RAR; ZO	4.855€	1.855€	38%
# 13	RAR	4.620€	3.620€	78%

The majority of the big savers – with a capital investment of less than 100.000€ - attribute more than 90% to development cost.

Concluding, although that significant portions of the investment budget are attributed to development the different participants agree that development cost for future DNSSEC deployments can significantly be reduced compared to the initial deployments. Leaders pay the bill, followers can limit their investments.

5.3 Cost of new features

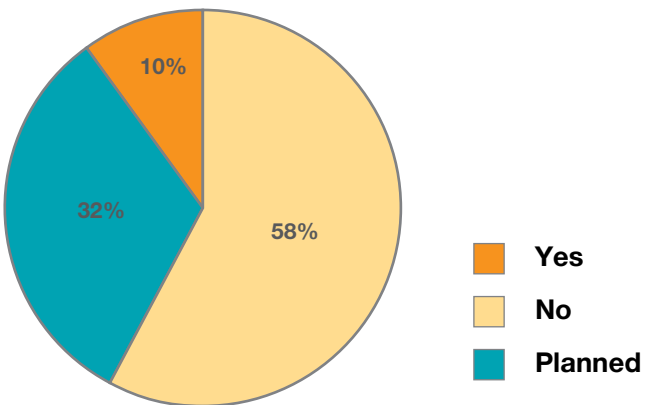
DNSSEC is still a changing technology, additional features or security improvements are still being added. The DNSSEC deployment of early adopters often doesn't support these new features or improvements (since they were not yet available at the time of deployment).

In the following section we discuss some of the additional features / security improvements of DNSSEC and how they were implemented by the participating organisations.

NSEC3

NSEC3 is an extension to DNSSEC which introduced a hashed authenticated denial of existence answer in the DNSSEC protocol. Through the stocktaking was identified that most organisations did not (yet) implement NSEC3.

Table 9 – **Use of NSEC3**



An important factor that needs to be taken into account here that NSEC3 has only recently been included in popular name server software (e.g. NSEC3 was included in BIND 9.6 in May 2008). Therefore not many organisations have

had the chance to include it in their DNSSEC deployment.

Through the stocktaking we identified two organisations who have already implemented NSEC3 (recently) and also a number of organisations who plan to implement NSEC3 in the future. As such, the cost for implementing NSEC3 is marginal.

DLV

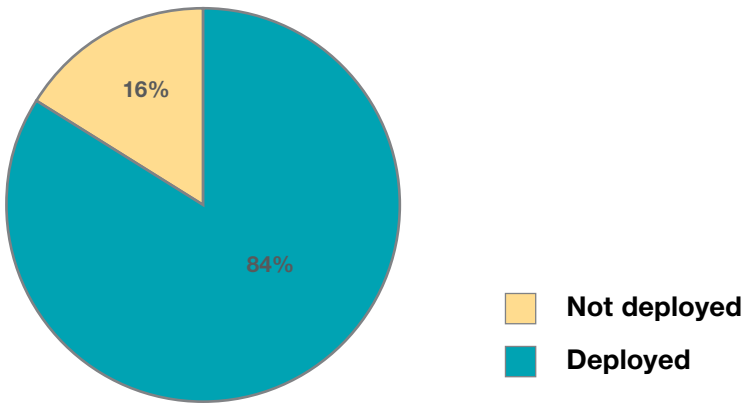
DNSSEC Look-aside Validation (DLV) is an extension to the DNSSEC protocol designed to assist in early DNSSEC adoption by simplifying the configuration of recursive servers.

Since - at the time of this writing - the root name servers have not yet been DNSSEC signed, alternatives such as DLV can be used to provide DNSSEC validation information.

Without DLV or a fully signed path from root to a zone, organisations and users would have to configure and maintain multiple trust keys in their configuration. This is an important factor to consider for recursive resolver operators since they are considered to be the most important trust anchor for end users.

Table 10 – **Use of DLV**

Stakeholder DLV Deployment Rate



DLV does not seem to be correlated with NSEC3. One registry and one zone operator and one recursive resolver operator have adopted DLV. Several interviewees indicated that their organisations preferred to wait for the root name servers to be signed (which is planned in the near future) instead of implementing DLV.

Those interviewees also indicated that the reason for not implementing DLV was the fact that – from a trust perspective - they did not like the idea of a single organisation being responsible for keeping the DLV records updated. The organisations which were reluctant towards implementing DLV also included several recursive resolver operators: these organisations took the decision to reduce the number of trusted zones they communicate with. They prefer to wait until the root name servers are signed before offering full DNSSEC validation.

Dynamic Update

Dynamic Update in DNS is a system in which changes to zone records are reflected in the name servers almost immediately after the change was made.

Dynamic Update is currently in use with only three out of the nine participants with more than 250 million DNS queries per day.

Table 11 – **Use of Dynamic Updates**

# ID	Role	Total Zones	Total Daily queries	Dynamic Updates
# 8	RAR; ZO	175.216	72.000.000	No
# 11	ZO; RRO	701	90.000.000	No
# 5	ZO	520	80.000.000	No
# 12	RAR; ZO	500	259.202.000	Yes
# 6	ZO	400	510	No
# 1	ZO	155	9.072.000.000	No
# 17	RAR; ZO	80	238.291.200	Yes
# 14	RY; ZO	45	3.750.000.000	No
# 13	ZO	20	648	No
# 9	RY; ZO	2	1.000.000.000.000	Yes

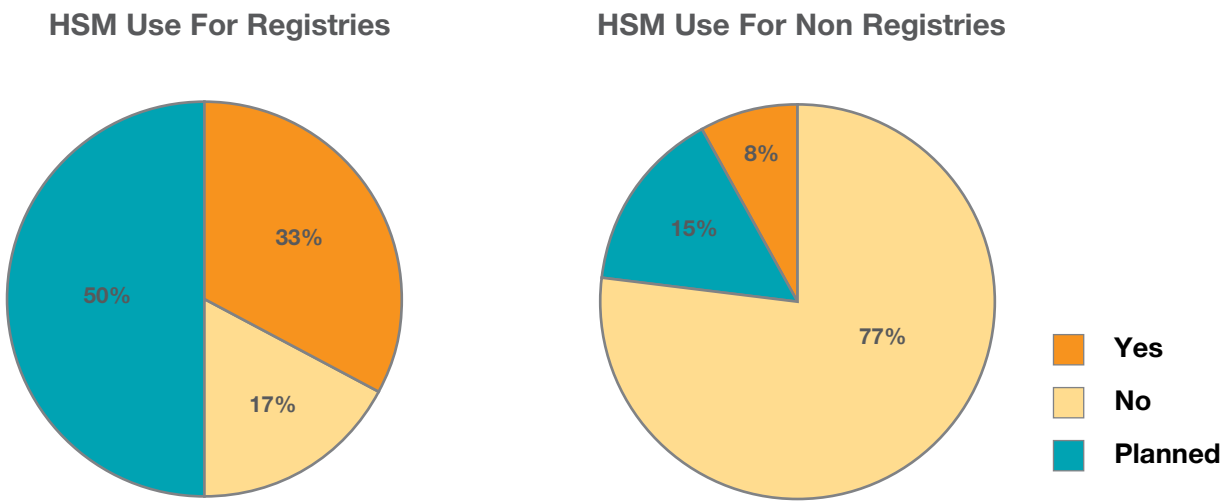
There seems to be no correlation between the amount of zones server, the total number of daily queries and the use of dynamic updates within the DNSSEC implementation of the interviewed organisations.

5.4 Key management cost

Key management is mainly a concern from registries and (reverse) zone operators. Most of them are looking into methods to automate key management processes. The limited involvement of pure registrars in key management is illustrated by the fact that registrars seem to adopt manual processes for the few key management actions that are part of their duty.

It is surprising to see that adoption of hardware security modules ("HSM's") is fairly limited in the DNSSEC community. Registries show an increased awareness of the importance and have concrete plans to use HSM in the near future. Contrary, organisations without a registry role tend to be less concerned and do not use – nor have plans to use – HSM's.

Table 12 – **Comparing use of HSM's between registries and non-registries**



One of the reasons for this seems to be the poor support of HSM within open source software. The OpenDNSSEC Project[11] - a cooperation of several organisations and individuals from the DNSSEC Community – aims at creating a turnkey solution to implement DNSSEC with better support for HSMs.

The size of the organization does not influence the choice on whether to use a HSM or not.

Respondents that have HSM technology in place recommend storing the private signing keys in a HSM to prevent compromise, theft or misuse of these keys. Such incident could jeopardize the complete security schema of DNSSEC and could negatively impact numerous internet applications. These respondents are concerned about their role in the authentication chain, starting with a known good trust anchor. Internet users rely on the trustworthiness of this trust anchor to prevent fraud and computer abuse.

Two out of five participants that already use HSM's in their key management procedures indicate an investment cost of less than 500€, which corresponds with a typical setup using smartcard technology. The other participant estimated the investment cost of the HSM to be higher.

Table 13 – **Cost for Hardware Security Module**

# ID	Role	HSM Cost
# 18	RY; ZO	25.000€
# 20	ZO; RRO	10.000€
# 8	RY	2.000€
# 2	ZO	400€
# 16	RY; RAR; ZO	100€

Concluding, the cost of key management is merely the cost of the HSM but rather the cost of developing and implanting the key management processes. Respondents included this cost in the overall deployment effort, making it impossible to measure this cost as a separate item.

"All stakeholders are very positive about their DNSSEC deployment and recommend others to follow."

5.5 Other costs

Throughout the interviews with the various stakeholders we enquired about other costs such as training and legal support. Most stakeholders indicated that they had a cost related to training, however no indication was given on the cost of the trainings or time spent on them, due to the fact that the budget for these training sessions comes out of the general training budget of an organisation.

With regards to legal support, only two organisations (both of them registries) indicated that they requested external legal assistance on the DNSSEC implementation. The required legal expertise has been mainly around the legal value of a signed DNS record and possible implications.

Again, no detailed cost figures have been received from the stakeholders for this type of support.

[11] http://www.opendnssec.org/

6 Analyzing Operational Expense

6 Analyzing Operational Expense

An operational expenditure (OPEX) is an on-going cost for running a product, business, or system.

Almost all of the participating organisations did not provide sufficient insight in the operational cost of DNSSEC operations. This could point toward an operational reality where the operational overhead of DNSSEC is smoothly integrated in existing operational costs.

The only operational cost aspect that was mentioned by some participants is the bandwidth.

6.1 Bandwidth cost

Increasing bandwidth is the only operational cost item where there seems to be an agreement between the different participants.

Table 14 – **Bandwidth increase versus portion of DNSSEC in resolver queries**

# ID	Role	Daily DNSSEC Queries	Daily Regular Queries	% of queries with DNSSEC	% in bandwidth increase
# 13	RY; ZO	1.250.000.000	2.500.000.000	33%	15 %
# 16	ZO	3.024.000.000	6.048.000.000	33%	50 %
# 15	RY	311.040.000	518.400.000	37%	50 %
# 14	RY	345.600.000	864.000.000	29%	100 %

Based on these responses it is possible to put forward a rule of thumb to calculate the expected bandwidth increase when implementing DNSSEC.

The potential root cause of this bandwidth increase is the size increase of the signed DNS records which are sent out by the name servers. Respondents indicated that due to the DNSSEC implementation they were obliged to use new methods for the transfer of zones between different name servers. (E.g. IXFR, (incremental) zone transfers in which only the new or changed records are transferred, instead of AXFR, (full) zone transfers in which the complete zone is transferred.

> *"We anticipated 30% bandwidth increase but it's worse. We see after deployment that bandwidth utilization has doubled"*

7 Analyzing Adoption of DNSSEC

7 Analyzing Adoption of DNSSEC

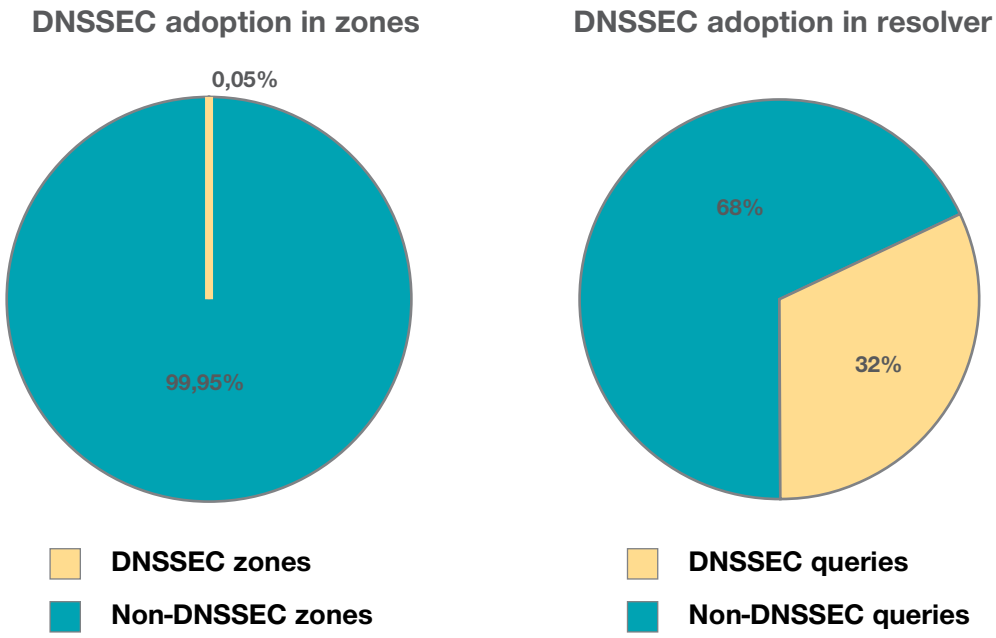
"Involve your marketing people early in your DNSSEC adventure; they can help spreading the message across"

This analysis makes a distinction between the adoption rates of signed zones as in DNSSEC capable top level domains and the adoption rates in the queries:

- The adoption rate in the top level domains (TLD's) gives an indication of the DNSSEC interest in the community of registrants, i.e. the customer of the survey's participants;
- the adoption rate in the queries gives an indication of the DNSSEC compatibility in the DNS resolvers querying the participant.

While the total number of signed zones is less than 1%, respondents reported that 32% of all resolver queries come from DNSSEC-aware resolvers.

Table 15 – **Adoption of DNSSEC in total of zones in top level domains versus total of resolver queries**



Based on the above illustration we can conclude that the DNSSEC adoption by DNS resolvers is at present more advanced than the adoption by registrants.

It shows clearly that the technological readiness for DNSSEC in name servers is much higher than the amount of actually signed zones within DNSSEC ready top level domains.

This should come as no surprise, since the supporting technical infrastructure should be in place before zones can be signed.

7.1 DNSSEC Signed Zones

In an attempt to better understand the dynamics of DNSSEC adoption by registrants, this study selected two countries for which both the ccTLD registry as well as subsequent registrars and zone operators participated in the survey.

Table 16 – **Countries with most developed DNSSEC adoption**

Country	Number of Participants	Total Zones in TLD	DNSSEC Zones in TLD	% of DNSSEC signed zones
A	3	925.216	1.574	0,170%
R	4	3.455.332	100	0,003%
T	4	1.388.922	3.812	0,274%

The above tables show that DNSSEC adoption by registrants is still very low. Participants indicated that the main reasons for this trend include:

- DNSSEC is still a fairly new technology, it is not known to all the end users;
- A few exceptions aside, DNSSEC is not an enforced requirement in DNS deployments. Currently users have to "opt-in" in order to use DNSSEC;
- There are still a number of end user operating systems and peripherals which are not DNSSEC compatible[12] or DNSSEC aware. In the second case, end users will not be signalled by their operating system or peripheral in case a DNSSEC validation failed or returned an invalid record. However, the recursive resolver they using will signal a DNS error;

Participants do not expect an explosive growth in the number of signed zones. Nevertheless, stronger growth is expected once the root name servers have been signed.

Table 17 – **% of DNSSEC capable queries**

# ID	Role	Daily DNSSEC Queries	Daily Regular Queries	%DNSSEC Capable
# 1	ZO	50.000.000	30.000.000	62.50%
# 17	ZO	259.200	388.800	40.00%
# 5	RY	311.040.000	518.400.000	37.50%
# 9	ZO	3.024.000.000	6.048.000.000	33.00%
# 13	RY; ZO	1.250.000.000	2.500.000.000	33.00%
# 19	RY;	345.600.000	864.000.000	28.57%

[12] Test Report: DNSSEC Impact on Broadband Routers and Firewalls [SAC035]. 16 September 2008 http://www.icann.org/en/committees/security/ssac-documents.htm.

The above table shows that on average 39% of all DNS queries are capable of DNSSEC. Furthermore we can conclude that organisations with a registrar role have the lowest adoption rate of DNSSEC zones versus total numbers of zones. This is as expected and less relevant.

Country view

Country A and Country T were selected due to their relatively high adoption rate of DNSSEC-enabled zones, with a percentage of 0,170% and respectively 0,274%.

Country T

The comparison of absolute figures of Country T highlights an interesting dynamic how DNSSEC can get adopted in a country. Participant #4 was the early adaptor and started DNSSEC deployment back in 1999. Under influence of this early adaptor, the ccTLD (participant #21) started to deploy DNSSEC in 2005. By setting the tone, the registry could convince two important registrars and zone operators to adopt DNSSEC over a period of two years. As a result, the country does now have a community where the complete value chain is enabled to handle DNSSEC.

Table 18 – **Adoption of DNSEC in Country T**

# ID	Role	Adopted DNSSEC Since	Total Zones	DNSSEC Zones
# 4	ZO	1999	400	200
# 21	RY; RAR; ZO	2005	888.122	1.862
# 6	RAR; ZO	2007	500.000	1.500
# 3	ZO	2007	400	250

Country A

The process that took place in Country A is significantly different from Country T. Instead of a gradual approach, three organisations in Country A decided in joint consultation to start deploying DNSSEC. Based on interviews with the involved participants this approach seems to be effective and sustainable.

Looking closer to the case of the latter, both the registry and an important registrar and zone operator simultaneously developed their DNSSEC capabilities.

Table 19 – **Adoption of DNSEC in Country A**

# ID	Role	Adopted DNSSEC Since	Total Zones	DNSSEC Zones
# 8	RY	2008	550.000	865
# 18	RAR	2008	200.000	13
# 15	RAR; ZO	2008	175.216	696

A common characteristic between both cases is that one organization combines the role of registrar and zone operator. It might be beneficial for DNSSEC adoption if there is an information exchange and common interest between the technical development of the zone operator and the promotion efforts from the registrants.

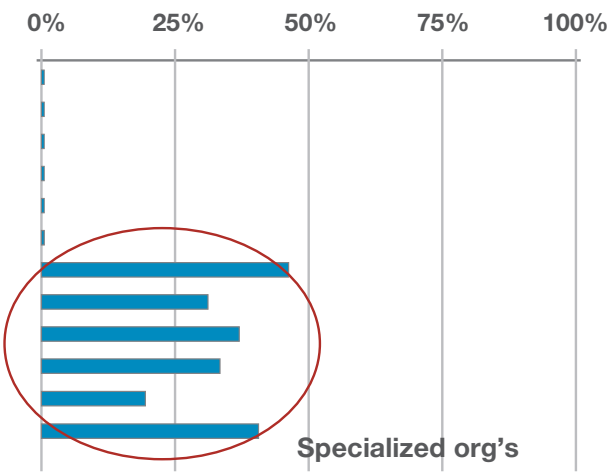
Specialization in DNSSEC

Table 20 – **Number of DNSSEC zones versus total of zones (absolute figures)**

# ID	Role	Total CAPEX Cost	Total Zones	DNSSEC Zones
# 15	RY; RAR; ZO	28.600€	888.122	1.862
# 13	RY	41.800€	550.000	865
# 20	RAR; ZO	6.575€	500.000	1.500
# 8	RAR	4.620€	200.000	13
# 6	RAR; ZO	4.855€	175.216	696
# 3	RAR; ZO	266.240€	80.000	10
# 20	ZO	22.617€	520	473
# 14	ZO	26.023€	400	200
# 7	ZO	5.100€	400	250
# 17	ZO	36.059€	155	85
# 19	RY; ZO	787.700€	45	10
# 1	ZO	335.590€	20	15

Table 21 – **Number of DNSSEC zones versus total of zones (relative figures)**

# ID	Total Zones	% of zones with DNSSEC
# 15	888.122	0,209%
# 13	550.000	0,157%
# 20	500.000	0,299%
# 8	200.000	0,006%
# 6	175.216	0,396%
# 3	80.000	0,012%
# 21	520	47,633%
# 14	400	33,333%
# 9	400	38,462%
# 17	155	35,417%
# 19	45	18,182%
# 1	20	42,857%



Comparing the relative figures of DNSSEC zones versus total of managed zones it becomes visible that all pure play zone operators host less than 600 zones. At least 20% of these zones are DNSSEC zones. This phenomenon might be an indication that the participating zone operators are recognized as a specialist in DNSSEC, and that they succeed to attract, convince or oblige domain owners to enable DNSSEC. Interesting enough, two out of the five big spenders are in this category of zone operators, which strengthens the idea of specialization.

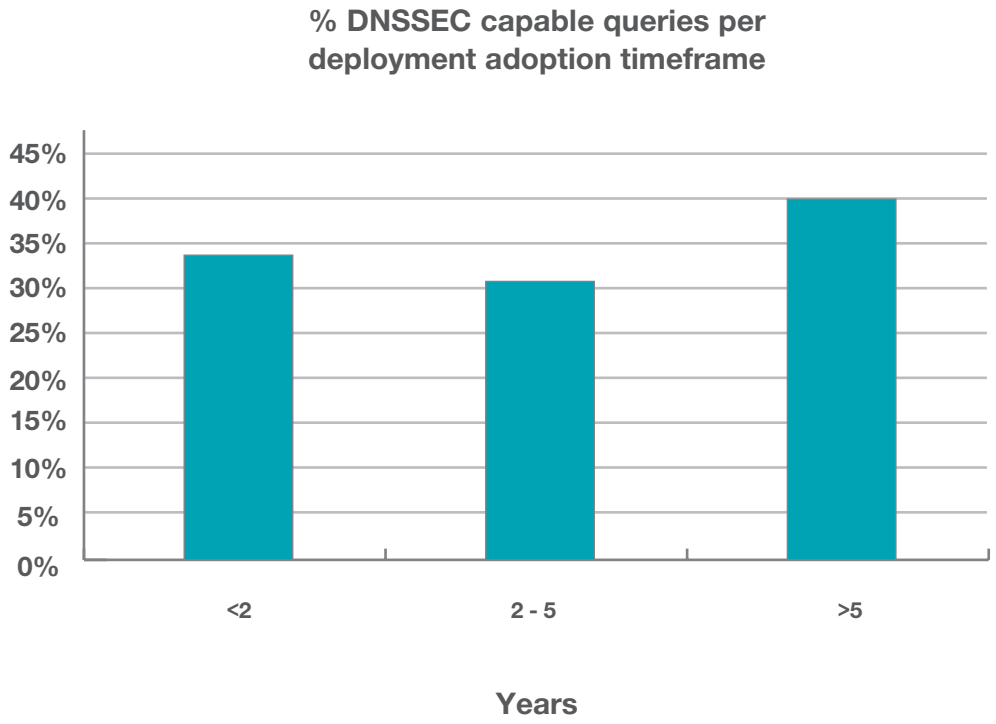
In contrast are all registrars with more than 80.000 zones to administer for which there are less than 1% DNSSEC enabled zones.

Only one of this category is currently testing DNSSEC and anticipates an investment of 266.000€.

7.2 DNSSEC queries

Based on the analysis of DNSSEC traffic out of the total DNS traffic an organisation generates, we noted that the amount of DNSSEC capable traffic (i.e. queries with the "DO-bit" set) varies from between the different organisations.

Table 22 – **% of DNSSEC capable queries per deployment adoption timeframe**



Based on the percentage of DNSSEC capable queries (meaning queries for which the DO bit is set), we can conclude that the longer an organisation has deployed DNSSEC, the more DNSSEC capable queries are generated. Furthermore, we noted that the last year a higher number of DNSSEC capable queries are generated as of the beginning of the deployment.

7.3 Cost Evolution

As DNSSEC adoption grows and technology and procedures related to DNSSEC become more standardized, the costs for newer deployments will decrease. Throughout the interviews, stakeholders indicated that for current deployments, the additional costs in a one and three year period will be minimal. Some small changes will need to be made to current deployments once the root name servers are signed, the costs of these changes will be insignificant.

For new deployments, the current development of out-of-the-box solutions such as OpenDNSSEC[13] will reduce the capital expense costs of a DNSSEC deployment to the cost of configuring an appliance.

> *"All stakeholders are very positive about their DNSSEC deployment and recommend others to follow."*

[13] http://www.opendnssec.org/

8 Analyzing Business Benefits

8 Analyzing Business Benefits

8.1 Registry

Business Trigger

The initiative for deploying DNSSEC in a zone often originates from the registry responsible for the zone.

Business Benefits

The main business benefit for a registry is the increasing security brought to the internet services by DNSSEC. Registrants want to provide assurance to the internet community that their zone is properly protected. Such assurance might have positive effect on market share and/or reputation of the registrant.

Registries feel that it is their responsibility to lead-by-example when it comes to the security of the DNS system. Registries use their own DNSSEC deployment to push their registrars and zone operators towards DNSSEC adoption. A practical method that proved to be successful is to involve registrars and zone operators in testing of the registry's DNSSEC deployment. Additionally, registries are eager to assist registrars and zone operators to set up their own DNSSEC capability and provide free-of-charge guidance and advice to them.

Note that most registries are non-profit organisations, so commercial targets and profit objectives are of minor importance.

Deployment parameters

Registries indicate that the deployment of DNSSEC is twofold:

- Technical development: Registries typically choose open source software and integrate it within their current environment;
- Operational development: Registries are typically aware of the importance of the non-technical aspects of DNSSEC as they look for answers on the following non-technical issues as well:
  - *Legal responsibility*: What is the legal value of a "signed" domain name? Would it uphold in a court of law as a valid legal signature for the information that was signed?
  - *Key management*: How will the cryptographic keys be protected during their key lifecycle: generation, distribution, use and termination? Can key management be supported by common multi-purpose operating systems or are dedicated hardware devices – such as HSM or Smartcard – required? How far can the key management processes be automated, is there a need for 4-eye protection during this process?

The survey revealed that organisation with a more mature IT Governance process tended to opt for formal key management procedures with several built-in controls while organisations with more informal processes tend to opt for the automated solutions.

8.2 Registrars

Business Trigger

Registrars often initiate their project for DNSSEC implementation once a TLD for which they are reselling domains starts to offer DNSSEC.

Business Benefits

Registrars might use DNSSEC as a differentiator that offers a competitive advantage. However, due to the fairly limited adoption of DNSSEC zones this benefit is still limited.

Most registrars offer DNSSEC as a "free security option" to their customers. The majority of the interviewed registrars combine their role with the role of (reverse) zone operator. Some of these registrars charge money for DNSSEC as an extra service (e.g. 2 € / domain / year).

Deployment parameters

DNSSEC implementation projects at registrars tend to be less costly and time consuming then similar project at registries or zone operators. The reason behind this is that registries will often guide registrars in their implementation; therefore less time has to be spent by the registrars on research on the technology.

Registrars tend to focus solely on the technical development of their administrative tooling to include DNSSEC as an attribute in their reselling process.

8.3 Zone Operators

Business Trigger

Zone operators are stimulated by at one end the registries that want to promote the use of DNSSEC, but at the other end by the registrants that want to use DNSSEC.

Business Benefits

Zone operators might use DNSSEC as a differentiator that offers a competitive advantage. However, due to the fairly limited adoption of DNSSEC zones this benefit is still limited.

We noted that some zone operators charge money for DNSSEC as an additional service. Average cost for registrants would be 2 € per year per domain. Although that none of the respondents answered that current revenue figures can bear the cost, further adoption of DNSSEC might anyhow generate additional revenue.

The big saver zone operators that also offer registrar services have deployed DNSSEC with a capital investment of less than 7 € per DNSSEC zone. Assuming that the adoption rate of DNSSEC zones would go up to 33% of total number of zones, it would mean that the capital expense per zone would drop to less than 0,08 € per zone for these operators. In such scenario, the zone operator might generate revenue if the use of DNSSEC is charged with margin to the domain owners. Key factor to make revenue with DNSSEC is the number of zones that are operated; large volumes of DNSSEC enabled zones make it possible to spread the investment cost and increase the income.

Deployment parameters

Zone operators tend to focus on technical development of the DNSSEC solution. The adoption of mature operational processes is less of a priority compared with the responses from registries.

8.4 Recursive Resolver Operator

Business Trigger

Recursive resolver operators are stimulated by the registries and end users to implement DNSSEC;

Business Benefits

The main business benefit for the recursive resolver operator would be the increased security of the DNS traffic handled by their name servers.

However through the interviews we saw that recursive resolver operators are reluctant to implement DNSSEC, most likely because that the financial benefits do not outweigh the implementation cost. Since that the majority of recursive resolver operators are commercial organisations – such as ISP's – this commercial barrier causes them to delay DNSSEC deployment as much as possible.

Deployment parameters

Recursive resolver operators tend to focus on technical development of the DNSSEC solution. The adoption of mature operational processes is less of a priority compared with the responses from registries.

8.5 Service Providers

Business Trigger

Current threats such as attackers trying to poison name server caches and the need to operate a secure environment are the main business triggers for service providers to start implementing DNSSEC.

Business Benefits

The main business benefit for the service provider would be the increased security of their name servers and their responses towards the end users.

Large service providers implementing DNSSEC face many challenges, including:

Upgrading a farm of 200+ name servers to DNSSEC capable technology is a major hurdle;

Operationalising DNSSEC in a name server farm supporting tens of thousands of domains of which the records are changed very often (daily for some domains);

Configuring the various trust anchors to link the different islands of trusts. For this DLV technology can be considered;

The key rollover and key management process;

Estimating the increase in resources (mainly bandwidth usage);

Additional challenge of implementing DNSSEC in a cloud environment;

Deployment parameters

Service providers not only tend to focus on technical development of the DNSSEC solution, they also take into account that they will have to adopt their operational processes to the use of DNSSEC, by adopting strict key management procedures for the DNSSEC related keys.

Appendix A: Overview of Stakeholders

Appendix A: Overview of stakeholders

This Appendix contains an alphabetical overview of all organisations which participated in the study. For each organisation, a short description on their activities has been included based on information obtained from their respective websites.

Active 24

Active 24 is a Pan-European provider of hosting services that focuses on small and middle enterprises. Active 24 provides them with complete and financially effective solutions for Internet, at the same time combining relevant, available and standardized products.

Website: www.active24.cz

Afilias

Afilias provides advanced registry services to several top level domains. Afilias began operations in July 2001 with the launch of the top-level domain registry for .INFO– the most successful of the seven new top-level domains (TLDs) selected by the Internet Corporation for Assigned Names and Numbers (ICANN) in 2001. Today, Afilias supports a more diverse base of TLDs than any other registry services provider and is the most experienced provider.

Website: www.afilias.info

Colt Telecom

COLT is a provider of Data, Voice and Managed Services to business and government in Europe. Customers of all sizes and working in all sectors rely on the extensive, secure and reliable network of Colt Telecom to deliver the higher performance they need from communications and IT systems.

Website: www.colt.net

Forpsi

FORPSI is a trademark which groups the webhosting, domain registration, server hosting and internet connection services of INTERNET CZ, INTERNET SK, AlphaNet and BlazeArts.

Their domain registration activity includes over 30 extensions and their full servicing includes DNS servers and redirecting.

Website: www.forpsi.com

Frobbit AB

Frobbit AB works actively with DNS and Internet since 1986 and deployed many technical standards which are used by the Internet today. Frobbit AB operates as registrar and offers DNS hosting services.

Website: www.frobbit.se

General Registry

General Registry is a registrar which operates the domainmaster platform. This platform allows registrants to register & manage national (.cz), generic (.com, .net, .org, .biz, .info, .name) and european (.eu) domain names.

Website: www.generalregistry.cz // www.domainmaster.cz

Internet Infrastructure Foundation

.SE (The Internet Infrastructure Foundation) is responsible for the top-level Swedish Internets domain, .se. The core business is the registration of domain names and the administration and technical operation of the national domain name registry, at the same time as .SE promotes the positive development of the Internet in Sweden.

When the new business model was introduced, March 9 2009, .SE divided current operations into two parts: .SE Registry and .SE Direkt. .SE Registry is responsible for administration and technical operation of the national domain name registry. Sales of domain names takes place through resellers called registrars. One of these is .SE Direkt, which is .SE's own registrar business.

Website: www.iis.se

IKS GMBH

IKS GMBH is an Internet Service Provider which offers commercial IT services. They attach importance to the security and integrity of the data of their customers.

Website: www.iks-jena.de

Interlan Gefle AB

The main business of Interlan Gefle AB is focussed around consulting in the areas of DNSSEC and IPv6. Interlan Gefle AB operates as zone operator and DNSSEC consultant.

Website: www.interlan.se

Loopia

Loopia is one of Swedens main webhosting and domain name registration providers. Since 2005 they are a part of the Mamut corporation. Mamut is a European provider of complete, integrated software solutions and internet services for SMEs. Mamut offers complete and user-friendly solutions at the best value for money integrating CRM, sales force, logistics, accounting, e-commerce, domains, e-mail, web hosting and security.

Website: www.loopia.se

Microsoft

Microsoft is a software vendor which offers creative solutions and services to business problems. They host websites for the different products and services (e.g. msn) they offer. In this context they manage a large number of domain name servers.

Website: www.microsoft.com

Neustar

Neustar provides the North American communications industry with essential clearinghouse services. Neustar operates the authoritative directories that manage virtually all telephone area codes and numbers, and enable the dynamic routing of calls among thousands of competing communications service providers (CSPs) in the United States and Canada. All telecommunications service providers (TSPs), as well as CSPs that offer telecommunications services to the public at large, must access the Neustar clearinghouse as one of their customers to properly route virtually all of their calls. Neustar also provides clearinghouse services to emerging CSPs, including Internet service providers, cable television operators, and voice over Internet protocol, or VoIP, service providers. In addition, they manage the authoritative directories for the .us and .biz Internet domains, as well as for Common Short Codes, part of the short messaging service, or SMS, relied upon by the U.S. wireless industry.

Website: www.neustar.biz

NIC cz

CZ.NIC, z. s. p. o., is an interest association of legal entities, founded in 1998 by leading providers of Internet services. The association currently has 63 members. The key activities of the association include operation of the domain name registry for the .CZ domain and the 0.2.4.e164.arpa (ENUM) domain, operation of the CZ top-level domain and public education in the area of domain names. The association is now intensively working on development of the ENUM system, extension and improvements of the domain administration system and support of new technologies and projects beneficial to the Internet infrastructure in the Czech Republic. CZ.NIC is a member of international organizations uniting similar organizations around the world (CENTR, ccNSO and more) and a member of the EURid association, managing the European domain .EU.

Website: www.nic.cz

Nominet

Nominet operates at the heart of e-commerce in the UK, running one of the world's largest Internet registries with over seven million domain names. With highly respected industry credentials, Nominet is entrusted with the management of the .uk and .44 registries, they employ 115 staff and have an annual turnover of £18m.

Website: www.nominet.org.uk

PIR

Created in 1984, .ORG is one of the internet's original top-level domains (TLDs), along with .COM, .NET, .GOV, .EDU and .MIL. Although it is "open" and "unrestricted", .ORG soon became the domain of choice for organizations dedicated to serving the public interest. The high regard of these well-intentioned organizations was soon conferred to this domain and today .ORG is considered by people around the world to be the domain of trust.

From small, local groups to huge, global foundations, a diverse range of noncommercial organizations use .ORG to advance their missions. Even many for-profit businesses use .ORG to gain support for their charitable activities.

In January 2003, the Public Interest Registry assumed responsibility for operating .ORG and maintaining the authoritative database of all .ORG domain names. (For more on the bid to manage .ORG, see ICANN.) The transition of .ORG from the previous operator to Public Interest Registry was the largest transfer in Internet history. More than 2.6 million domains were transferred in about a day, without affecting any .ORG registrant or website.

Website: www.pir.org

RIPE NCC

The RIPE NCC is an independent, not-for-profit membership organisation that supports the infrastructure of the Internet through technical co-ordination in its service region. The most prominent activity of the RIPE NCC is to act as the Regional Internet Registry (RIR) providing global Internet resources and related services (IPv4, IPv6 and AS Number resources) to members in the RIPE NCC service region. The membership consists mainly of Internet Service Providers (ISPs), telecommunication organisations and large corporations located in Europe, the Middle East and parts of Central Asia.

Website: www.ripe.net

Stichting Internet Domeinnamen

SIDN is responsible for the functional stability and development of the .nl Internet domain. As well as registering and allocating .nl domain names, the organisation enables Internet users all over the world to make use of these labels at any given moment. SIDN's rapidly growing domain name register now contains more than three million .nl domain names, which are the subject of almost one million successful searches a day. In consequence, SIDN is a key player in the global Internet community. The organisation's services are provided to the public through a network of two thousand independent commercial Internet service providers. SIDN also plays an active role in the technical, regulatory and political development of the Internet, at the national and international levels. Through the ENUM Foundation for the Netherlands, SIDN is additionally at the forefront of preparations to bring ENUM to the Netherlands. Formed in 1996, SIDN is based in the Dutch town of Arnhem, where it employs fifty people.

Website: www.sidn.nl

Stichting NLnetlabs

NLnet Labs is a research and development group that focuses on those developments in Internet technology where bridges between theory and practical deployment need to be built; areas where engineering and standardization takes place.

It is their goal to play an active and relevant role in these areas through the development of open source software, through participating in development of open standards, and through the dissemination of knowledge.

Website: www.nlnetlabs.nl

SURFnet

SURFnet is a subsidiary of the SURF organisation, in which Dutch universities, universities for applied sciences and research centres collaborate nationally and internationally on innovative ICT facilities. SURFnet enables groundbreaking education and research. SURFnet designs and operates the hybrid SURFnet6 network and provides innovative services in the field of security, authentication and authorisation, group communication and video.

Website: www.surfnet.nl

Telia Sonora

Telia offers a comprehensive range of telecommunication services in Sweden. Telia focuses on businesses, consumers and organizations and is market leader in Sweden for these product areas: mobile communications, fixed voice, data communications and broadband.

Website: www.telia.se

Visiant outsourcing

Visiant Outsourcing is an IP Infrastructure & IT Strategic Outsourcer, which plans and realizes solutions to satisfy the more specific requirements in IT Outsourcing, Business Continuity & Disaster Recovery, Internet & Intranet Publishing and the distribution of network based applications.

Website: www.visiantoutsourcing.it

Appendix B: Survey Questionnaire

Appendix B: Survey Questionnaire

Contact information

Details of the organisation

Name:

Roles in DNS organisation (mark all that apply):

☐ Registry ☐ Registrant ☐ Reverse Zone Operator

☐ Registrar ☐ Zone Operator ☐ Other:

Country:

Website (url) for this entity:

Staff employed in your organisation (please complete using FTE14) :

ADMINISTRATIVE STAFF	Nr. of FTE
Junior (1 – 4 year relevant experience)	
Senior (4 – 10 year relevant experience)	
Master (10+ year relevant experience)	
TECHNICAL STAFF	**NR. OF FTE**
Junior (1 – 4 year relevant experience)	
Senior (4 – 10 year relevant experience)	
Master (10+ year relevant experience)	

Details of the contact person

Family name:

First name:

Job Title:

Company Address:

Country:

Email:

Telephone:

[14] Full Time Equivalent

DNSSEC Implementation

Status of DNSSEC Implementation within the organisation:

☐ DNSSEC in production

☐ DNSSEC test bed

☐ Considered DNSSEC, no implementation or test track yet

If DNSSEC was considered, please indicate when your organisation plans to start testing/implementing:

☐ Discontinued DNSSEC implementation

How many internet facing DNSSEC-capable name servers are being operated by your organisation? (Please specify in number of boxes)

☐ IPv4 nameservers

☐ IPv6 nameservers

Did the number of internet facing DNSSEC-capable name servers increase due to the implementation of DNSSEC? If so, please explain the main reasons for expanding the capacity.

The following question is only applicable to registries and zone operators:

How many zones are served – as primary zones - by these name servers?

☐ zones of which ☐ zones are signed with DNSSEC.

The following question is only applicable to zone operators:

Please provide us with an indication on the (average) size of the zone(s) served:

◯ <100.000 records

◯ 100.000 <1.000.000 records

◯ >1.000.000 records

How many queries (in total) do these internet facing name servers receive on average on a daily basis ?

DNSSEC Queries: ☐

Regular DNS Queries: ☐

The following question is only applicable to registries:

Could you provide us with contact information of registrars, registrants or zone operators which are also implementing DNSSEC under your signed top level domain and could be interested in participating in this survey.

Cost of implementation phase (capex)

We would like to ask you to complete this section with the exact cost figures from the DNSSEC project in your organisation. In case the DNSSEC implementation project is not yet started or still in progress, estimates can be used rather than experience figures.

The cost of implementation has been divided into three project *phases*, being development, test and deployment.

The Development phase consists of all activities necessary to develop, acquire, and configure DNSSEC up to and including training.

The Test phase consists of all activities to ensure correct and reliable operation that are performed between the Development phase and the actual go-live of the deployment.

The Deployment phase starts when DNSSEC becomes operational.

For each *phase* in the implementation project, a subsection has been created in this questionnaire in order to obtain a detailed overview of the different costs in each phase. Please note that the costs in these sections are additional costs (eg. costs of development don't need to be taken into account when completing the "test" section).

Due to the sensitivity of some information, we understand if it would not be possible to share all detailed cost information (e.g. cost per man-day of employees). However, if this information could be shared it will be greatly appreciated since it will lead to a better outcome of this study.

Furthermore, if this section could not be completed in the required detail, please mention this in section 2.1.4 and provide us with an overview of the overall cost and a description what is included in those costs figures.

DEVELOPMENT PHASE

Lead time of the development phase: ☐

Please indicate here how many working days have passed between the start and end of the development phase.

Human Resources

Please indicate in the table below which types of resources are required for a successful development of a DNSSEC implementation. Please make a clear distinction between internal & external resources as well as the different roles these resources may have (developers, system administrators, ...)

Following list can be used as a reference for assigning experience levels:

- Junior : 1 to 4 years of relevant experience;
- Senior: 4 to 10 years of relevant experience;
- Master: 10+ years of relevant experience;

Due to the sensitivity of some information, we understand if it would not be possible to share all detailed cost information (e.g. cost per man-day of employees). However, if this information could be shared it will be greatly appreciated since it will lead to a better outcome of this study.

TYPE OF RESOURCE	EXPERIENCE LEVEL	MANDAYS REQUIRED	COST PER MANDAY (EUR)	TOTAL COST (EUR)

Infrastructure Costs

Short description of system hardware used/made available for development:

DNSSEC related purchase cost of these systems: [ ] EUR

Please note that in case these systems are also used for other developments, this should be taken into account when nothing down the purchase cost of these systems. In these cases, only the partial cost of the hardware purchase should be taken into account for this questionnaire. This question also includes the required network infrastructure required to interconnect the various systems and protect them from outside threats

Operating cost of the infrastructure during the development phase: [ ] EUR

This includes costs such as housing, electricity, air conditioning, ...

Comparing the required infrastructure with the infrastructure required for the existing situation, the organisation has noted an increase of: (please complete)

[ ] % increase in hardware costs during the development phase

[ ] % increase in operating cost of this infrastructure during the development phase

Software Costs

Short description of software licenses required for the development:

DNSSEC related purchase cost of these licenses: [ ] EUR

Please note that in case this software is are also used for other developments, this should be taken into account when nothing down the purchase cost of these licenses. In these cases, only the partial cost of the license purchase should be taken into account for this questionnaire.

Comparing the required software with the software required for developing the regular DNS system, the organisation has noted an increase of: (please complete)

[ ] % increase in software costs during the development phase

Other Costs

Please provide an overview of other costs related to the development of DNSSEC within the organisation. This could include training, legal advice, (security) audits by external organisations, etc. Please indicate those costs either in EUR and/or in cost increase factor against regular DNS (in %).

Have other initiatives been introduced in combination with DNSSEC (eg. IPv6)? In this case, how much investments / effort (in %) has been in common with the DNSSEC investment?

☐ %

Is a HSM (Hardware Security Module) being used to store the DNSSEC keys? If so, what was the cost related to the purchase and use (e.g. custom software) of this HSM?

☐ EUR

TEST PHASE

Lead time of the test phase: [ ]

Please indicate here how many working days have passed between the start and end of the test phase.

Human Resources

Please indicate in the table below which types of resources are required for a successful testing of the DNSSEC development. Please make a clear distinction between internal & external resources as well as the different roles these resources may have (developers, system administrators, ...)

Following list can be used as a reference for assigning experience levels:

- Junior : 1 to 4 years of relevant experience;
- Senior: 4 to 10 years of relevant experience;
- Master: 10+ years of relevant experience;

Due to the sensitivity of some information, we understand if it would not be possible to share all detailed cost information (e.g. cost per man-day of employees). However, if this information could be shared it will be greatly appreciated since it will lead to a better outcome of this study.

TYPE OF RESOURCE	EXPERIENCE LEVEL	MANDAYS REQUIRED	COST PER MANDAY (EUR)	TOTAL COST (EUR)

Infrastructure Costs

Short description of system hardware used/made available for testing:

DNSSEC related purchase cost of these systems: [ ] EUR

Please note that in case these systems are also used for other test exercises, this should be taken into account when nothing down the purchase cost of these systems. In these cases, only the partial cost of the hardware purchase should be taken into account for this questionnaire. This question also includes the required network infrastructure required to interconnect the various systems and protect them from outside threats.

Operating cost of the infrastructure during the testing phase: [ ] EUR

This includes costs such as housing, electricity, air conditioning, ...

Comparing the required infrastructure with the infrastructure required for testing the existing situation, the organisation has noted an increase of: (please complete)

[ ] % increase in hardware costs during the test phase

[ ] % increase in operating cost of this infrastructure during the test phase

Software Costs

Short description of software licenses required for the test environment:

DNSSEC related purchase cost of these licenses: [ ] EUR

Please note that in case this software is are also used for other test exercises, this should be taken into account when nothing down the purchase cost of these licenses. In these cases, only the partial cost of the license purchase should be taken into account for this questionnaire.

Comparing the required software with the software required for testing the regular DNS system, the organisation has noted an increase of: (please complete)

[ ] % increase in software costs during the test phase

Other Costs

Please provide an overview of other costs related to the testing of the DNSSEC implementation within the organisation. This could include training, legal advice, (security) audits by external organisations, etc. Please indicate those costs either in EUR and/or in cost increase factor against regular DNS (in %).

IMPLEMENTATION PHASE

Lead time of the implementation phase: ☐

Please indicate here how many working days have passed between the start and end of the implementation phase.

Human Resources

Please indicate in the table below which types of resources are required for a successful implementation of DNSSEC. Please make a clear distinction between internal & external resources as well as the different roles these resources may have (developers, system administrators, ...)

Following list can be used as a reference for assigning experience levels:

- Junior : 1 to 4 years of relevant experience;
- Senior: 4 to 10 years of relevant experience;
- Master: 10+ years of relevant experience;

Due to the sensitivity of some information, we understand if it would not be possible to share all detailed cost information (e.g. cost per man-day of employees). However, if this information could be shared it will be greatly appreciated since it will lead to a better outcome of this study.

TYPE OF RESOURCE	EXPERIENCE LEVEL	MANDAYS REQUIRED	COST PER MANDAY (EUR)	TOTAL COST (EUR)

Other Costs

Please provide an overview of other costs related to the implementation (move to production) of DNSSEC within the organisation. This could include training, legal advice, (security) audits by external

organisations, etc. Please indicate those costs either in EUR and/or in cost increase factor against regular DNS (in %).

Cost of operations (opex)

Human Resources

Please indicate in the table below which types of additional resources are required for successfully operating the DNSSEC infrastructure (vs. the regular DNS environment). Please make a clear distinction between internal & external resources.

Following list can be used as a reference for assigning experience levels:

- Junior : 1 to 4 years of relevant experience;
- Senior: 4 to 10 years of relevant experience;
- Master: 10+ years of relevant experience;

Due to the sensitivity of some information, we understand if it would not be possible to share all detailed cost information (e.g. cost per man-day of employees). However, if this information could be shared it will be greatly appreciated since it will lead to a better outcome of this study.

TYPE OF RESOURCE	EXPERIENCE LEVEL	MANDAYS REQUIRED	COST PER MANDAY (EUR)	TOTAL COST (EUR)

Infrastructure Costs

Please describe below a short description of the hardware in the production environment. Also note whether a capacity plan has been created for operating the DNSSEC infrastructure. Describe the expected increase in capacity and the associated costs (per year) due to DNSSEC deployment:

Annual hardware costs: ☐ EUR

Annual supporting operating costs (housing, electricity, ...): ☐ EUR

Required connectivity (bandwidth): ☐

Annual connectivity costs: ☐ EUR

Comparing the required infrastructure with the infrastructure required for operating the existing DNS system, the organisation has noted an increase of: (please complete)

☐ % increase in hardware costs

☐ % increase in operating cost of this infrastructure

☐ % increase in bandwidth usage

☐ % increase in connectivity cost

Other Costs

Please provide an overview of other annual costs related to the operation of DNSSEC within the organisation. This could include training, legal advice, (security) audits by external organisations, etc. Please indicate those costs either in EUR and/or in cost increase factor against regular DNS (in %).

Interview questions

Based on the information provided through the above questions, an interview will be scheduled in the form of a phone conference in order to elaborate further on certain aspects such as:

Commercial Value

- What where the main business drivers for deploying DNSSEC?
- What are the expected gains or advantages of DNSSEC over "regular" DNS?
- How does the organisation rate their own DNSSEC deployment: what have been the successes and what are the points for improvement?
- How long is DNSSEC being supported by the organisation?
- How many (in%) of your customers are using DNSSEC? What are your future predications/expectations of this number? (growth, stagnation, ...)

DNSSEC Deployment Project: Planning & Execution

- The projection of changes required for the deployment of DNSSEC in one year and three year's time;
- How the organisation is currently operating DNSSEC (under an unsigned root, island of trust, ...), what would be the (financial) impact and level of change required to change the current DNSSEC operations to operate e.g., under a signed root;
- Have specific parts of the deployment project been outsourced to third parties? If this was the case: which parts and what was the associated cost;
- For DNS Registries: on the above questionnaire, an overview has been given on development costs. How big a part of these costs are used to adapt the current administrative interfaces to include DNSSEC key management;
- What type of DNSSEC implementation has been considered/implemented in the organisation: default installation or use of additional features such as NSEC3, DLV, dynamic updates, ...
  Where there specific costs involved?
- Has your organisation:
  - Attended conferences with regards to DNSSEC?
  - Collaborated with other organisations (in the broad sense so including registries, registrars, registrants & zone operators) which were also deploying DNSSEC?
  - Exchanged software with other organisations which were also deploying DNSSEC? How did this impact the deployment costs?
- Did you encounter unexpected situations or aspects while implementing DNSSEC? Which?
- Looking back, what would the organisation do differently when deploying DNSSEC (lessons learned)?
- What would you advise to other organisations who are considering to deploy DNSSEC?

DNSSEC Deployment Project: Technical

- Did custom development occur to enhance or expand the features and functionality of DNSSEC? If so, what are the benefits/improvements? What was the impact on the cost of deployment?
- Who is performing the key management of the KSK (Key Signing Key) and ZSK (Zone Signing Key)?

Appendix C: Data Gathering Aproach

Appendix C: Data Gathering Approach

Stocktaking methodology

In order to conduct the stocktaking, Deloitte applied its Survey Methodology in order to support the engagement team in execution and delivery of the tasks requested to obtain feedback on the cost assessment of DNSSEC deployment.

Deloitte's Survey Methodology adopts a three-stage approach for the collection of detailed information, as graphically depicted in the figure below. Firstly, we identify the target groups, key stakeholders and the relevant contact persons within these.

As part of the questionnaire development exercise and in line with ENISA expectations, the questionnaire was tested in pilot phase with a small number of elected stakeholders to assess the effectiveness and completeness of the questionnaire.

Approach

The approach used in this stocktaking engagement consisted of the following phases:

1. Identify target group and key stakeholders

Different stakeholders were identified based on the contacts from both ENISA and the DNSSEC Workgroup as well as the Deloitte network. The intention was to obtain stakeholders in each of the following roles:

- Registry
- Registrar
- Registrant
- Zone Operator
- Recursive Resolver Operator

Stakeholder Sample Selection

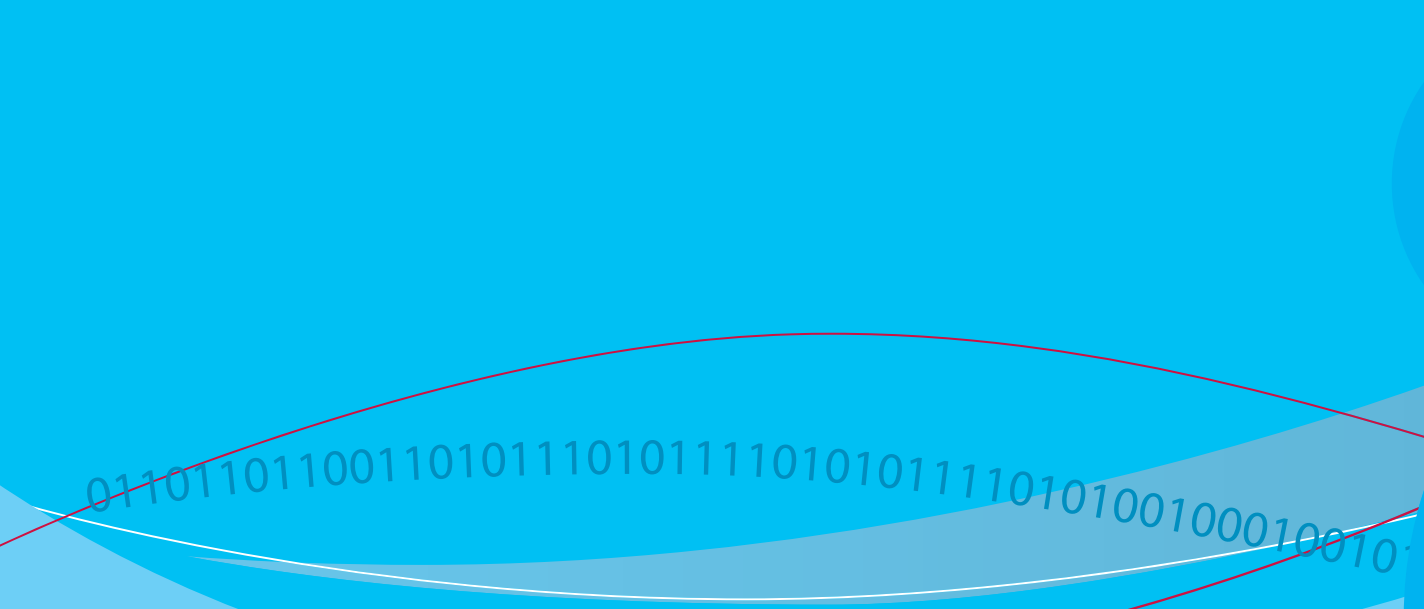
Stakeholders were selected to have a more or less equal amount of the above roles represented in the final sample selected for the study. Furthermore, stakeholders which were known to have already implemented DNSSEC were given priority to be included in the sample.

Throughout the stocktaking exercise, additional stakeholders were added to the sample based on referrals from interviewees and additional contact data received from ENISA.

Data Quantification

Two methods have been used to quantify the data obtained through the stocktaking exercise:

- Quantify based on size of organisation (based on the numbers of domains/zones managed by the organisation):
- Quantify based on exposure and popularity of the organisation's name servers (based on the number of (dnssec) name server queries received on a daily basis.



enisa
European Network and Information Security Agency

P.O. Box 1309 71001 Heraklion - Crete - Greece
Tel: +30 28 10 39 1280, Fax: +30 28 10 39 1410
Email: resilience@enisa.europa.eu