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.