The costs of DNSSEC deployment

survey results

Panagiotis Saragiotis, ENISA

ccNSO members meeting @ICANN no. 38

Drivers for the study

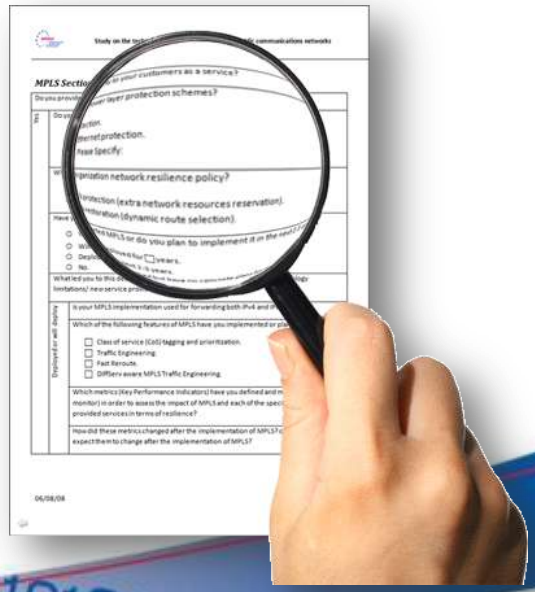
- Deploying a new technology requires investment
  - Hardware
  - Software
  - Human Resources
  - Bandwidth
- For DNSSEC these costs are not well defined
  - Uncertainty can hinder its deployment

Why ENISA?

- "Improving Resilience in European e-Communication Networks", 2008-2010
  - DNS is a critical service for IP Based Networks
  - Not designed to be secure
    - "Intentional omissions include security", Dr. Paul Mockapetris
  - Its improved stability and security will improve networks resilience
  - DNSSEC greatly enhances networks resilience. Policies and guidelines are needed

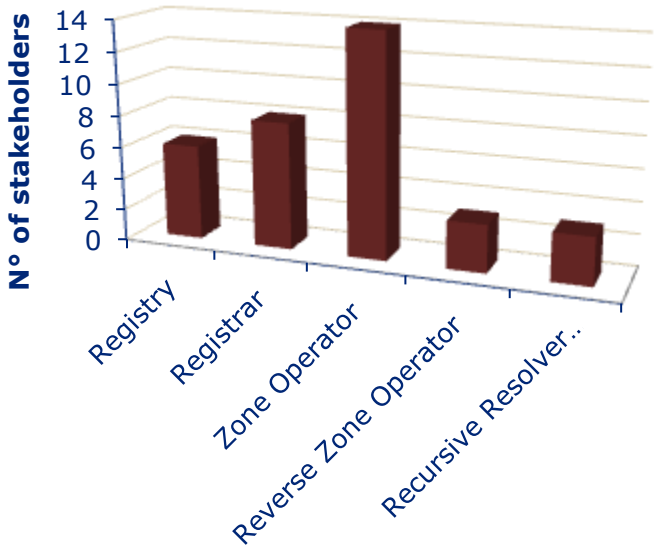
Objectives & Scope

- Objectives
  - Study the costs (CAPEX/OPEX) of DNSSEC deployment
  - Assess the required changes on resources of the different roles and operations
- Scope
  - Registries, Registrars, Zone Operators and Recursive Resolver Operators.
- Means
  - Stocktaking, questionnaires and interviews
- Side effects
  - Analyse adoption
  - Analyse business benefits
- Hurdles
  - Not detailed answers

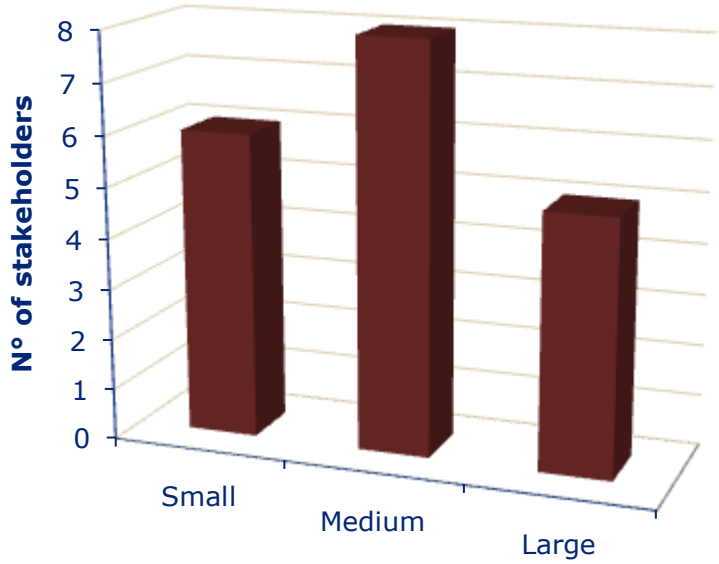


Stakeholders involved

Roles Surveyed



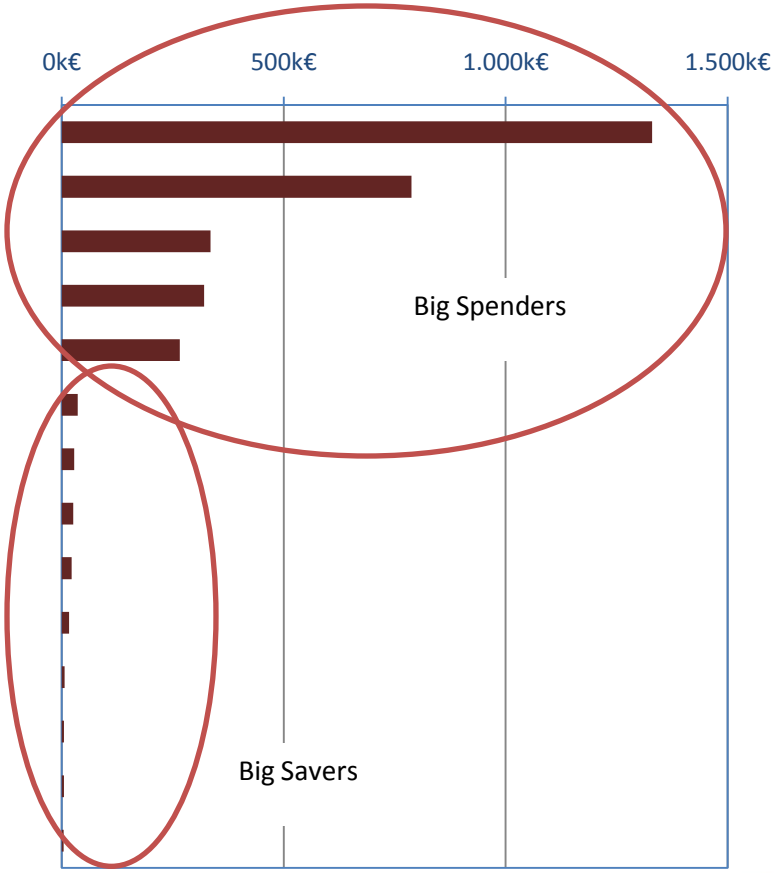
Stakeholder size in Terms of Zones



- Selection Criteria
  - Considered, implemented or abandoned a DNSSEC implementation
- Voluntary participation
- Timeframe
  - June to September 2009

Overall Investment Cost

- Clear distinction between "*big savers*" and "*big spenders*"
  - "big savers" invest on average 27.000€
  - "big spenders" invest on average 608.000€
- Pure play registrars
  - Investment cost below 5.000€



Big Spenders vs. Big Savers

Infrastructure costs

- Significant investments
  - 17% to 48% of total investment cost
- Use existing infrastructure
  - <10.000 €

Strategic Positioning

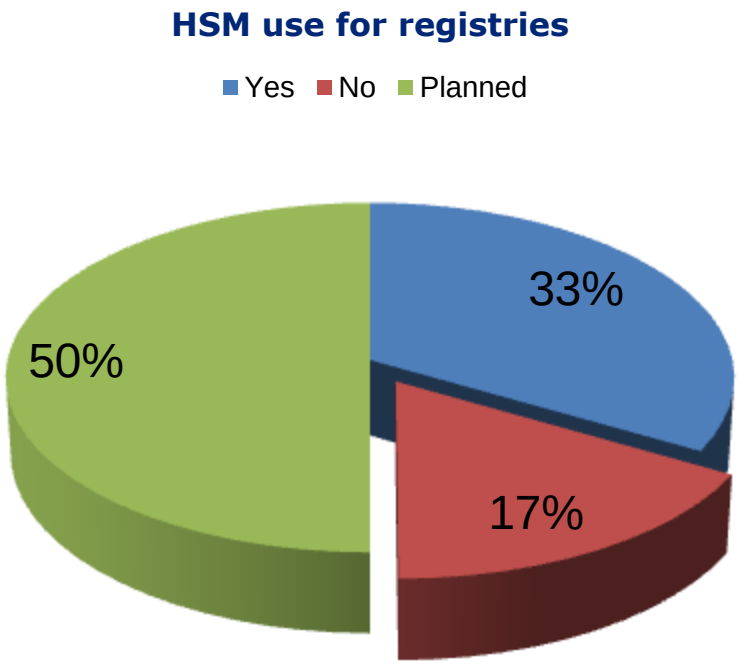
- Frontline of deployment
- Emphasis in governance
  - Key management
  - Operational processes
- Use existing open source software
- Limit themselves to customisations
  - 90% of cost

Software Cost

- Almost none of the correspondents have bought a commercial-of-the-shelf product
  - 83% use opensource
- Software costs come from:
  - in-house development
  - customization of open source solutions
- Early adaptors (before 2008) were obliged to invest significantly in in-house development
- Development cost for future DNSSEC deployments can significantly be reduced
  - “Leaders pay the bill, followers can limit their investments.”

Key Management Costs

- Only a limited number of stakeholders adopt hardware security modules (HSM's)
  - Poor support of HSM within open source software is one of the reasons
  - Size of the organisation does not influence the choice to implement HSM or not
- Costs vary between 500€ and 25.000€



Other Costs

- Deployment of specific features
  - NSEC3, Dynamic Updates, DLV
- Training
- Legal support
  - Legal value of a signed DNS record

Operational Expense

- Increasing bandwidth is the only operational cost item
  - Increase in zone size
  - Obliged to use new methods for the transfer of zones

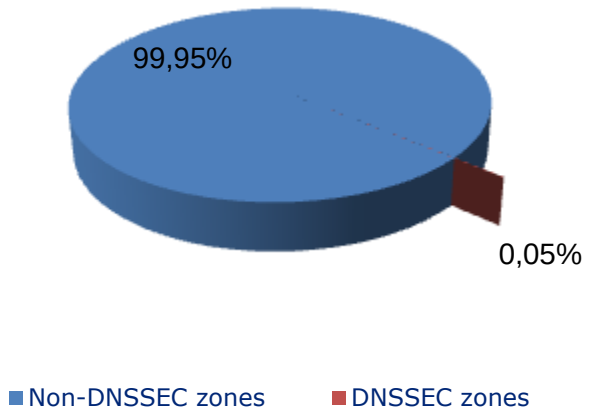
# ID	Role	Daily DNSSEC Queries	Daily Regular Queries	% of queries with DNSSEC	% in bandwidth increase
# 13	RY; ZO	1.250.000.000	2.500.000.000	33%	15 %
# 16	ZO	3.024.000.000	6.048.000.000	33%	50 %
# 15	RY	311.040.000	518.400.000	37%	50 %
# 14	RY	345.600.000	864.000.000	29%	100 %

Cost Evolution

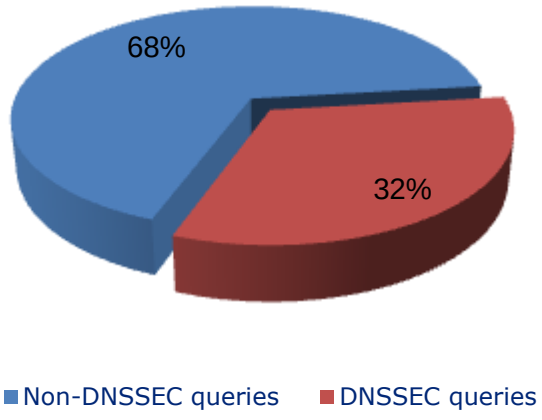
- Costs for newer deployments will decrease
  - As adoption grows and technology and procedures related to DNSSEC become more standardized
  - Out-of-the-box solutions will reduce the capital expense costs
- Additional costs in a one and three year period will be minimal
  - Costs of new features or adaption to new procedures (e.g. Signed Root)

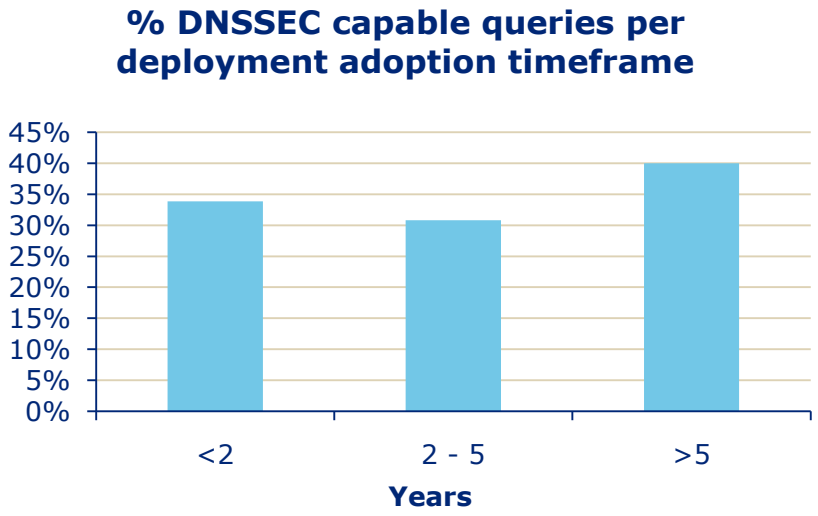
Adaption of DNSSEC

Signed Zones



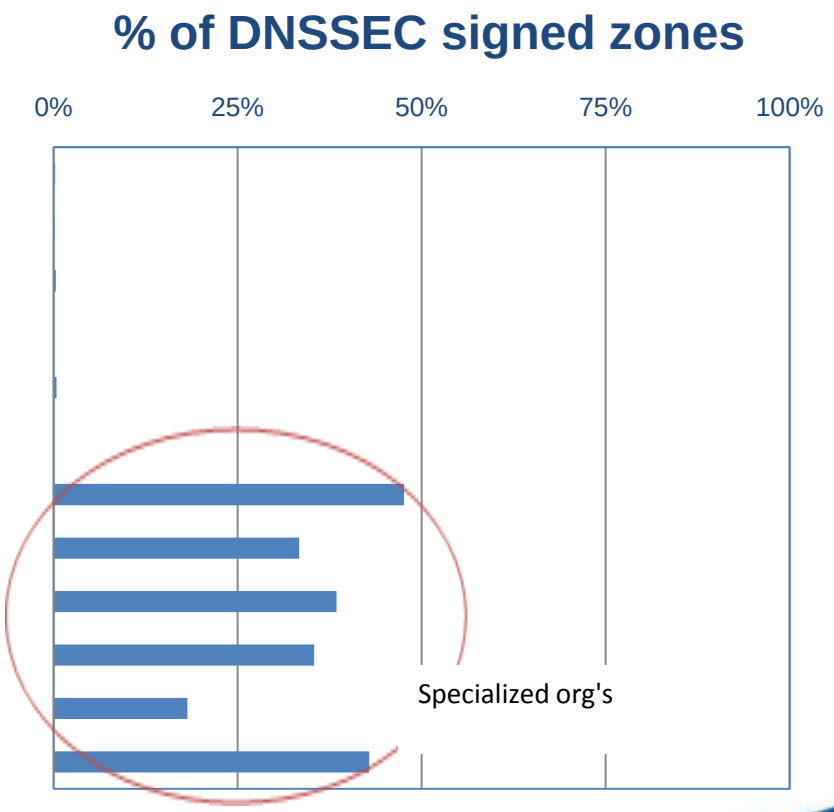
Resolver Queries





Specialization on DNSSEC

- Zone operators that deployed DNSSEC have an average of 30% of zones signed
- Host less than 600 zones
- Succeed to attract, convince or oblige domain owners to enable DNSSEC



Business Benefits and Motivation

- Registry
  - Become a reliable Trust Anchor
  - Lead by example and stimulate parties further down in the chain to adopt DNSSEC
  - Earn recognition in the DNS community
- Zone operator
  - Provide assurance to clients 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
- Registrar
  - Differentiator and competitive advantage versus others
- Recursive Resolver Operator
  - Assure end-users on DNS reliability and trustworthiness
  - Offering differentiator and competitive advantage

Good practices guide for deploying DNSSEC

GPG for deploying DNSSEC

- Addressed to:
  - Information security managers
  - Defining requirements for deployment
- Recommendations on security details and procedures
  - signing of a domain's zone;
  - providing validating recursive resolver services;
  - writing a DNSSEC practices statement;
  - selecting products or outsourcing services.

Just a few hints from the guide

- Before deploying DNSSEC
  - You created a DNS zone and forgot about its existence
  - Assumptions in the systems and the flexibility allowed zones with mistakes to operate
- When deploying DNSSEC
  - Signatures and keys have a validity period
    - Procedures have to be in place to update them in a timely manner
    - before DNSSEC time was relevant, now it is absolute
  - Zones should be tested for correctness using available tools enhancing the quality of the DNS

Online resources

- The costs of DNSSEC deployment
  http://www.enisa.europa.eu/act/res/technologies/tech/costs-of-dnssec-deployment

- Good Practices Guide for Deploying DNSSEC
  http://www.enisa.europa.eu/act/res/technologies/tech/gpgdnssec

- Technologies for resilience
  https://www.enisa.europa.eu/act/res/technologies