

DNSSEC activities of ENISA

Panagiotis Saragiotis
TF-CSIRT Technical Seminar

Why ENISA?

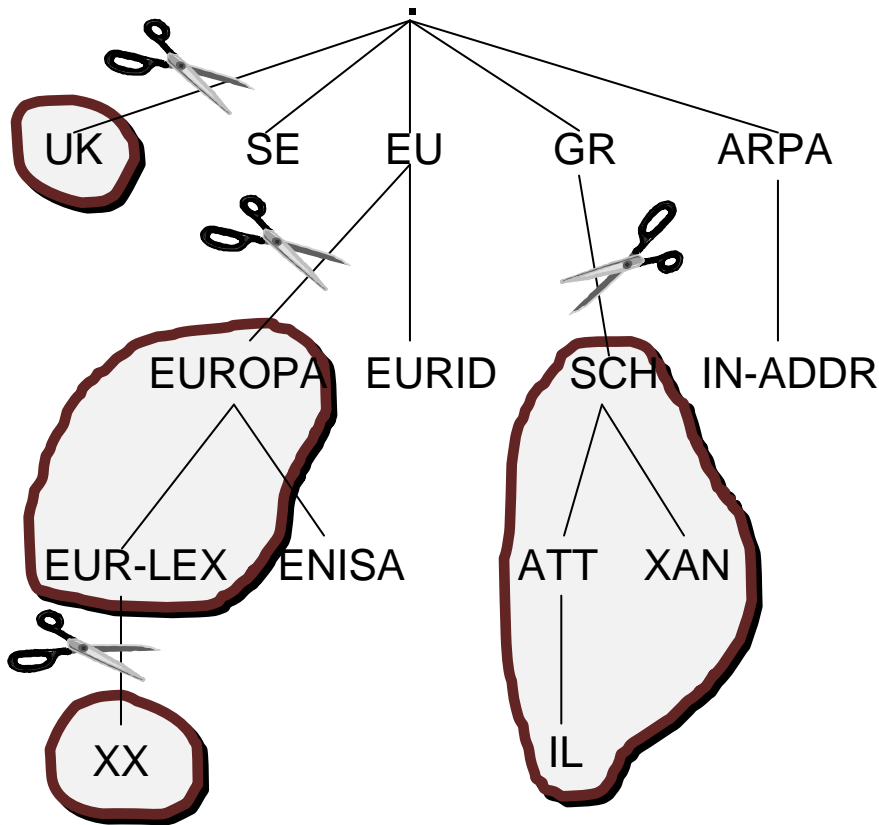
- ★ “Improving Resilience in European e-Communication Networks”, 2008-2010
 - ★ DNS is a critical service for IP Based Networks
 - ★ Not designed to be secure
 - “Intentional omissions include security”, Dr. Paul Mockapetris
 - ★ Its improved stability and security will improve networks resilience
 -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

About Resilience

- ★ Resilient are the networks that provide and maintain an acceptable level of service in face of faults affecting their normal operation.
- ★ The main aim of the resilience is for faults to be invisible to users.
- ★ Improving the resilience of a network is an issue of risk management which includes :
 - ★ risk identification;
 - ★ evaluation and;
 - ★ acceptance or mitigation.
- ★ A wide accepted list of risks to the resilience of networks includes :
 - ★ flash crowd events
 - ★ cyber attacks
 - ★ outages of other support services
 - ★ natural disasters and
 - ★ system failings
- ★ The mitigation of identified risks involves technical measures such as :
 - ★ resilient design
 - ★ resilient transmission media
 - ★ resilient equipment and
 - ★ technologies that improve resilience

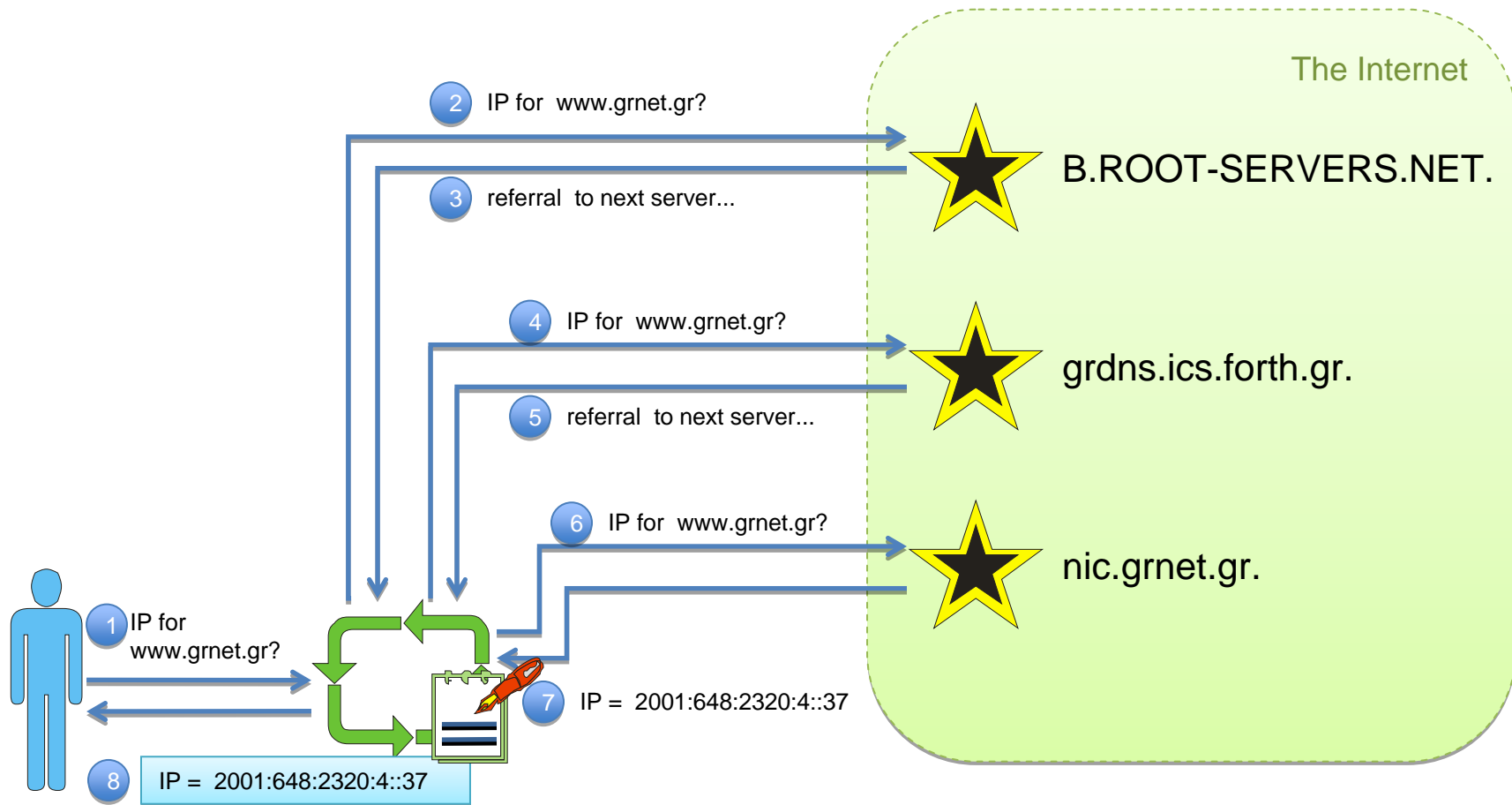


DNS a Hierarchical name space



- ★ A domain or zone can be as small as a single name
- ★ A domain or zone could be as large as the entire namespace
- ★ Each domain or zone can be identified by its topmost node
- ★ A name server that has a copy of some zone is said to be *authoritative* for that zone

Looking up a name 3/many



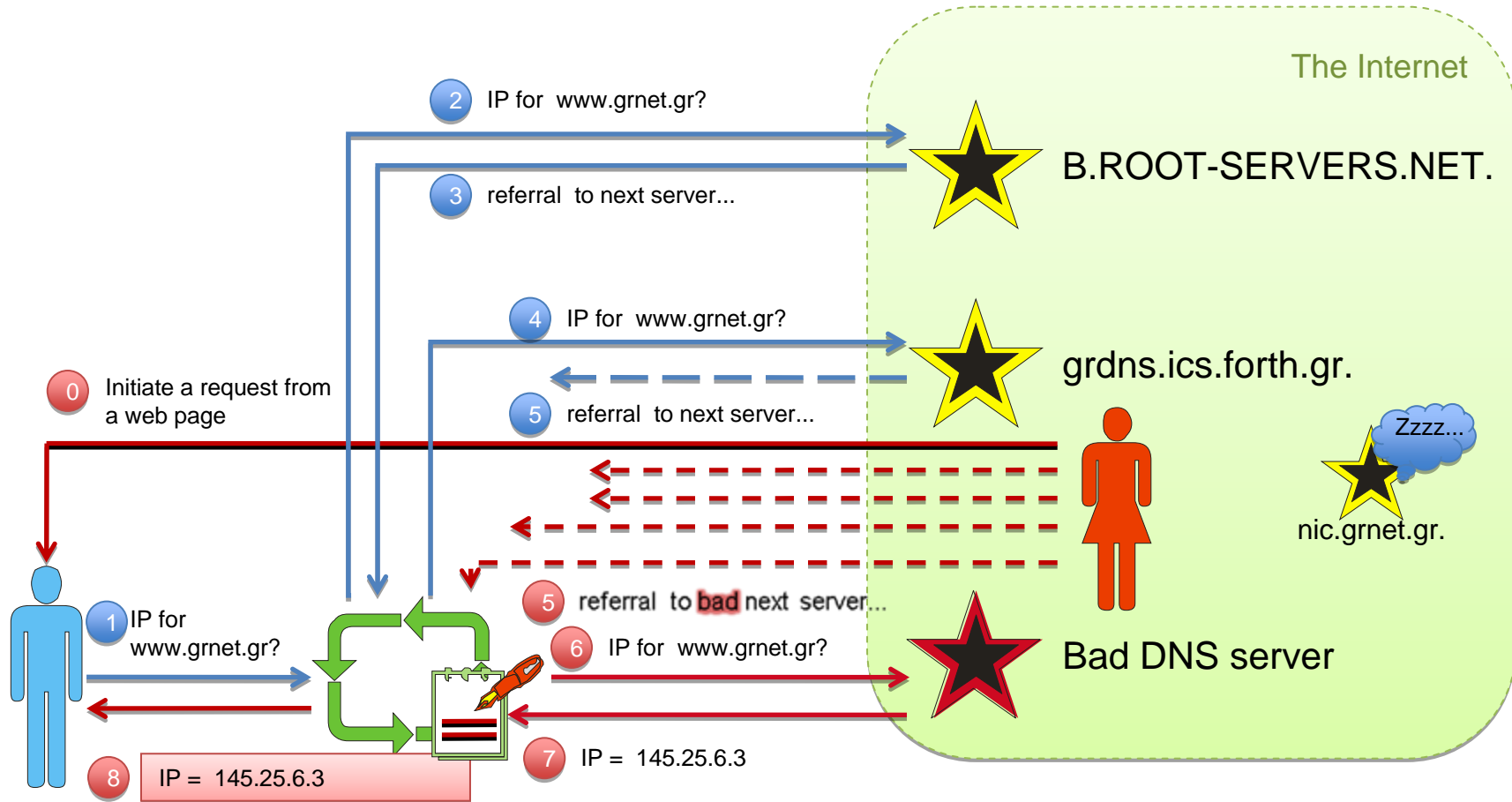
Looking up a name last/many

- ★ This procedure goes on under the hood
 - ★ Completes in just a split second
- ★ Distributed Database
 - ★ No one machine knows everything
- ★ Nothing prevents any nameserver from hosting any zone
 - ★ But, no one delegates to it

Known Threats

- ★ DNS Known Threats (RFC 3833)
 - ★ Packet Interception - man-in-the-middle attacks
 - ★ ID Guessing and Query Prediction
 - ★ Name Chaining - Cache Poisoning
 - ★ Betrayal By Trusted Server
 - ★ Denial of Service
 - ★ Wildcards

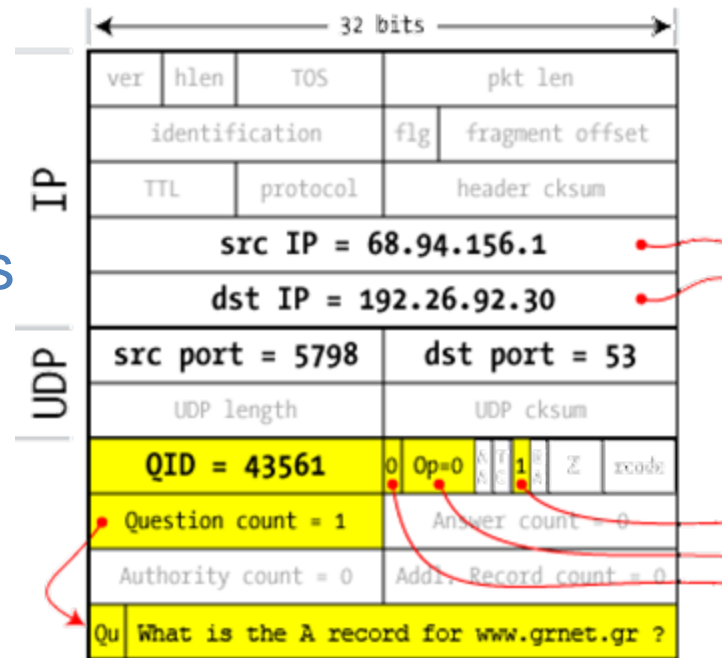
Cache poisoning 1/2



Protection ?

- ★ UDP port + QID
- ★ UDP port used to be standard
 - ★ Now it is in a range of thousands
- ★ QID was sequential
 - ★ Now it is random

$$\underbrace{2^{16}}_{\text{Source ports}} \times \underbrace{2^{11}}_{\text{Query ID}} = 2^{27} = \mathbf{134 \text{ million}}$$



- ★ Even with randomization, Evgeniy Polyakov, proved to have achieved cache poisoning in 10 hours, using two computers and gigabit LAN.

DNSSEC

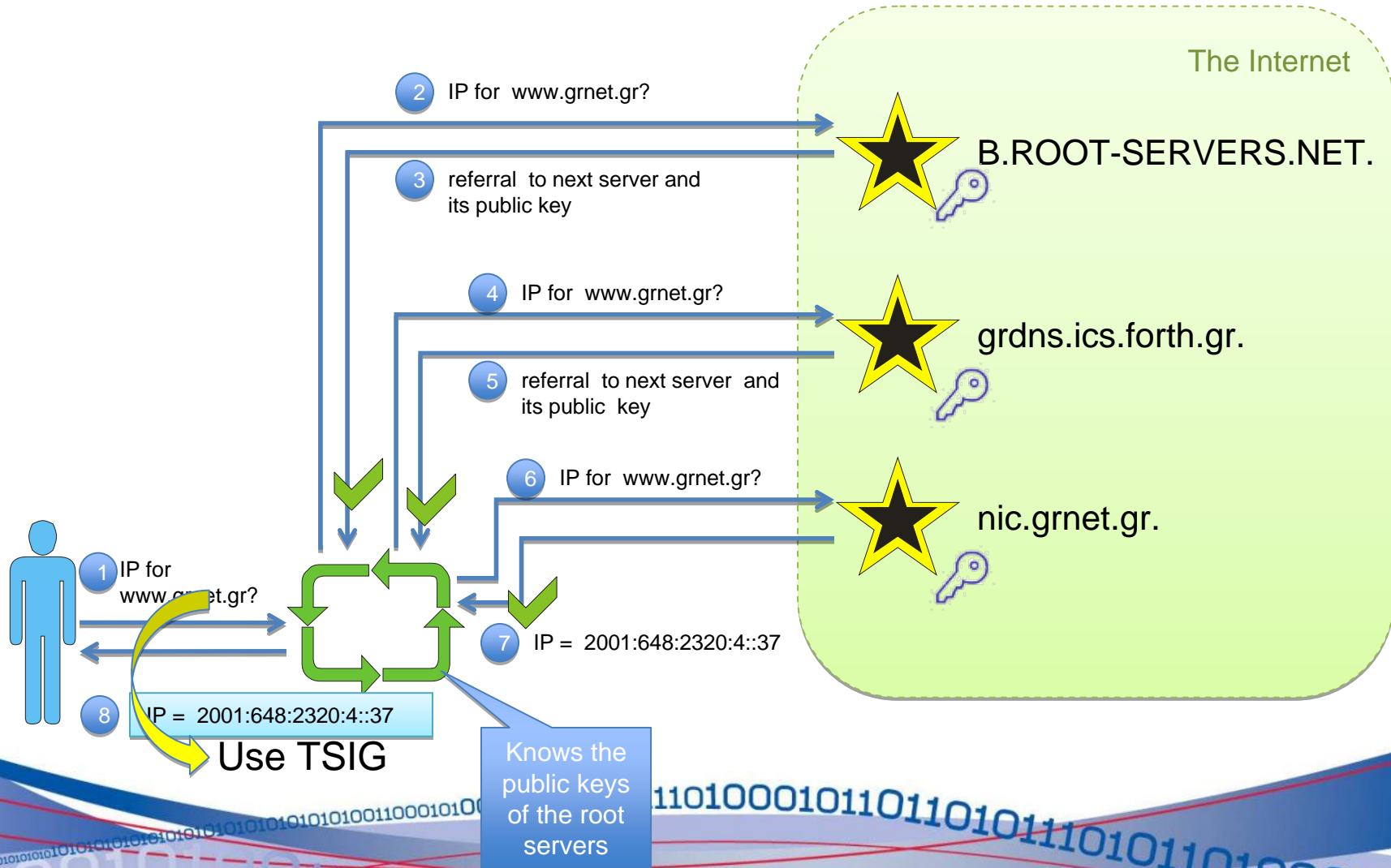
★ DNSSEC features

- ★ End-to-end data integrity check.
- ★ DNS data origin authentication.
- ★ Authenticated denial of existence.

★ What It doesn't provide

- ★ Confidentiality
- ★ Stub Client to Resolver security
 - Use TSIG to ensure the integrity with a recursive name server

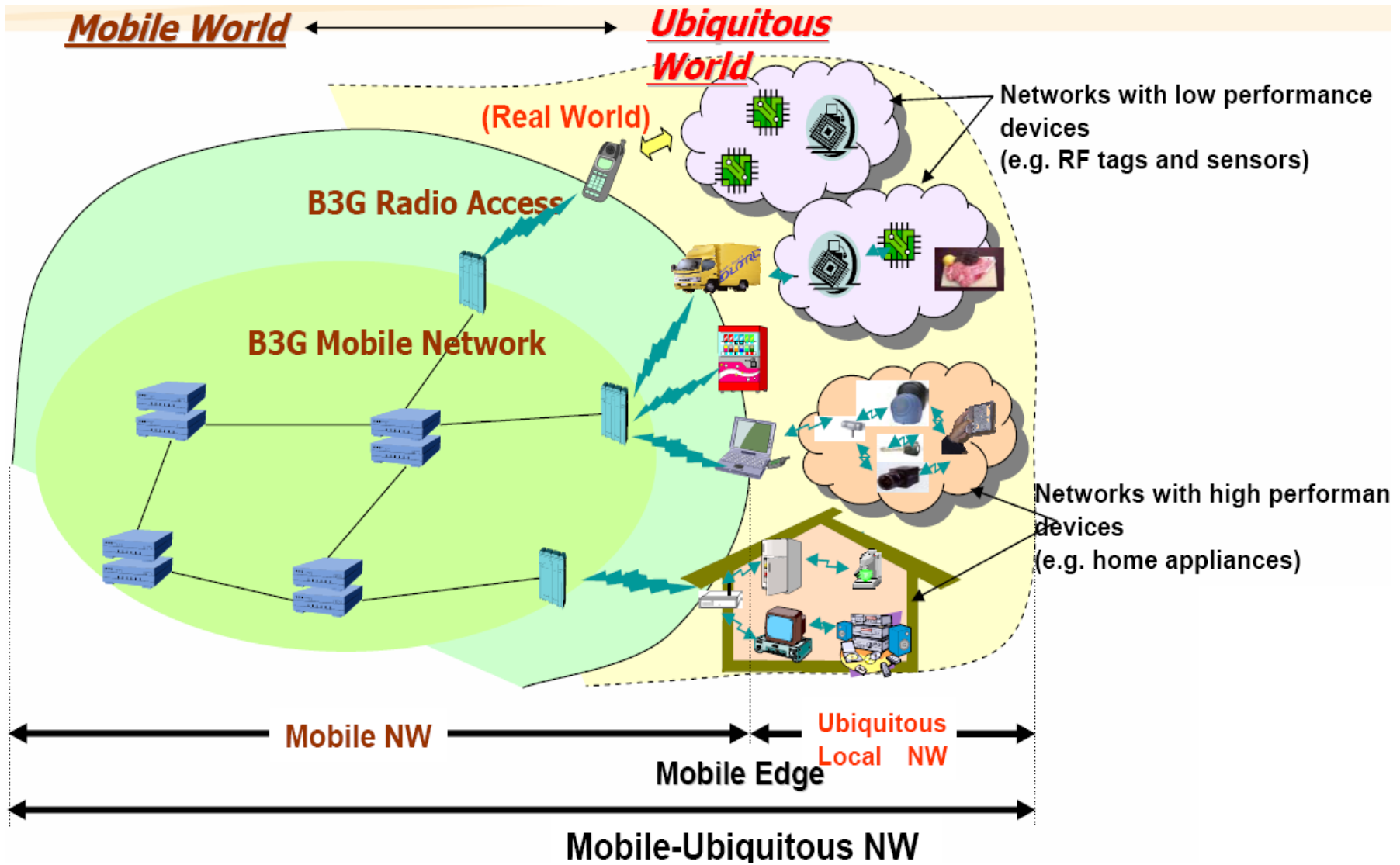
Looking up with DNSSEC



DNSSEC Weaknesses

- ★ Answer validation increases the resolver's work load.
- ★ New ways for Denial of Service.
- ★ Trust model is almost totally hierarchical.
- ★ Key rollover at the root is really hard.
- ★ Zone Walking
 - ★ Solved with NSEC3
- ★ Betrayal By Trusted Server still exists as threat.

Future Networking Trends



DNSSEC activities of ENISA

★ 2008

- ★ Survey Deployment Status;
- ★ Paper on the security features and the problems it solves;
- ★ Stocktaking operators on the perceived security enchantments.

★ 2009

- ★ Study costs of deployment;
- ★ Good Practice Guide on deploying DNSSEC.

★ 2010

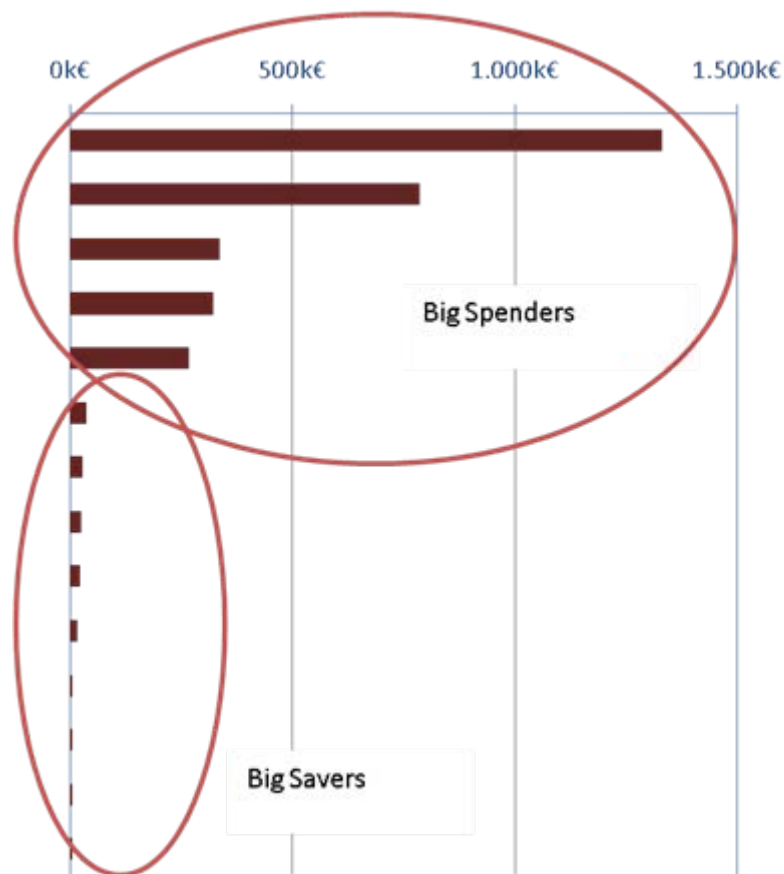
- ★ Pilot actions;
- ★ Create end user // educational // promotional material.

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

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

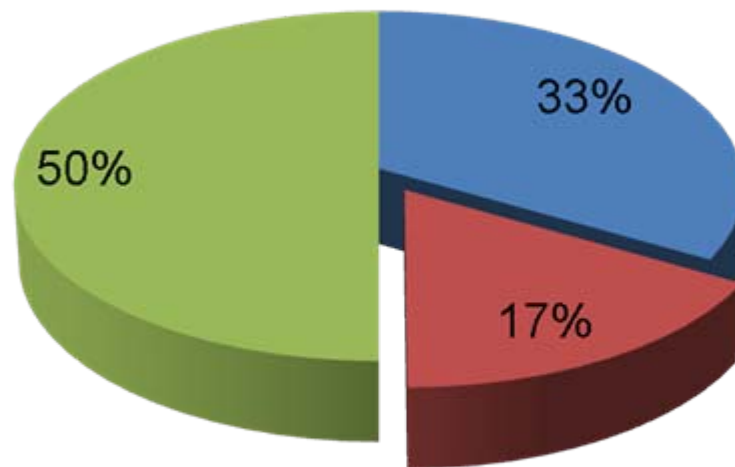
- ★ Almost none of the correspondents have bought a commercial-of-the-shelf product
 - ★ 83% use opensource
- ★ Software costs come from:
 - ★ in-house development
 - ★ customization of open source solutions
- ★ Early adaptors (before 2008) were obliged to invest significantly in in-house development
- ★ 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€

HSM use for registries

■ Yes ■ No ■ Planned



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
 - ★ Obligated to use new methods for the transfer of zones

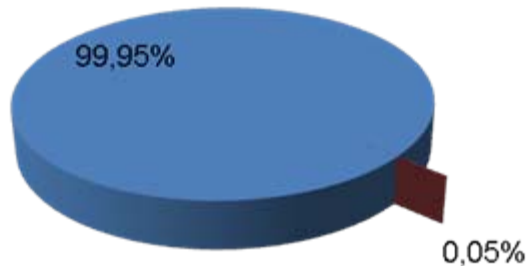
# ID	Role	Daily DNSSEC Queries	Daily Regular Queries	% of queries with DNSSEC	% in bandwidth increase
# 13	RY; ZO	1.250.000.000	2.500.000.000	33%	15 %
# 16	ZO	3.024.000.000	6.048.000.000	33%	50 %
# 15	RY	311.040.000	518.400.000	37%	50 %
# 14	RY	345.600.000	864.000.000	29%	100 %

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)

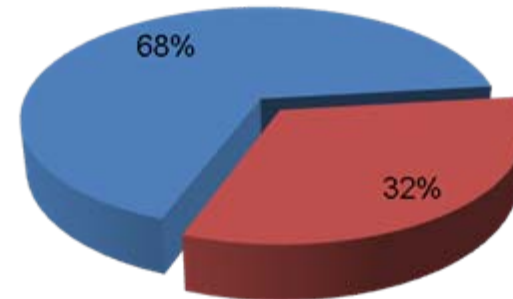
Adaption of DNSSEC

Signed Zones



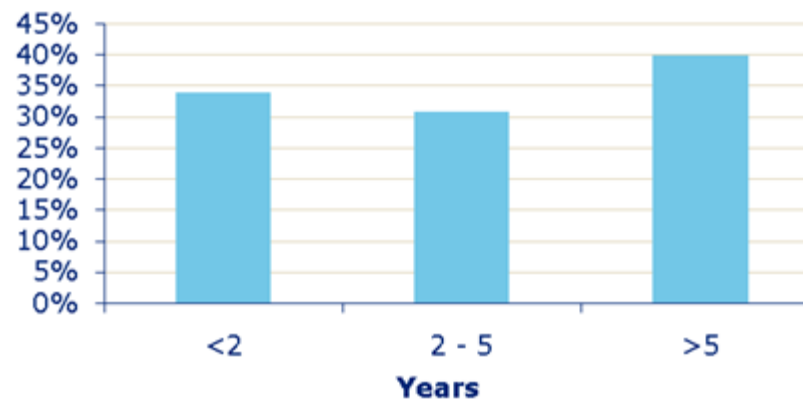
■ Non-DNSSEC zones ■ DNSSEC zones

Resolver Queries



■ Non-DNSSEC queries ■ DNSSEC queries

% DNSSEC capable queries per deployment adoption timeframe



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

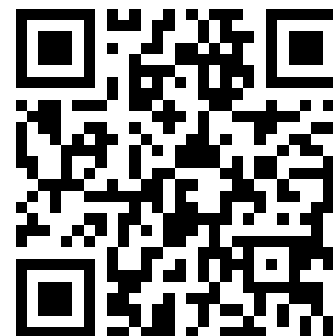
- ★ Assure end-users on DNS reliability and trustworthiness
- ★ Offering differentiator and competitive advantage



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

Video on Importance of Resilience



<http://www.youtube.com/user/enisasta>