The Real cost of Implementing DNSSEC for a Registry

Luis Diego Espinoza
IT Advisor NIC – Internet Costa Rica
ICANN 38 – Brussels, June 2010

.cr
NIC-Internet Costa Rica
Academia Nacional de Ciencias

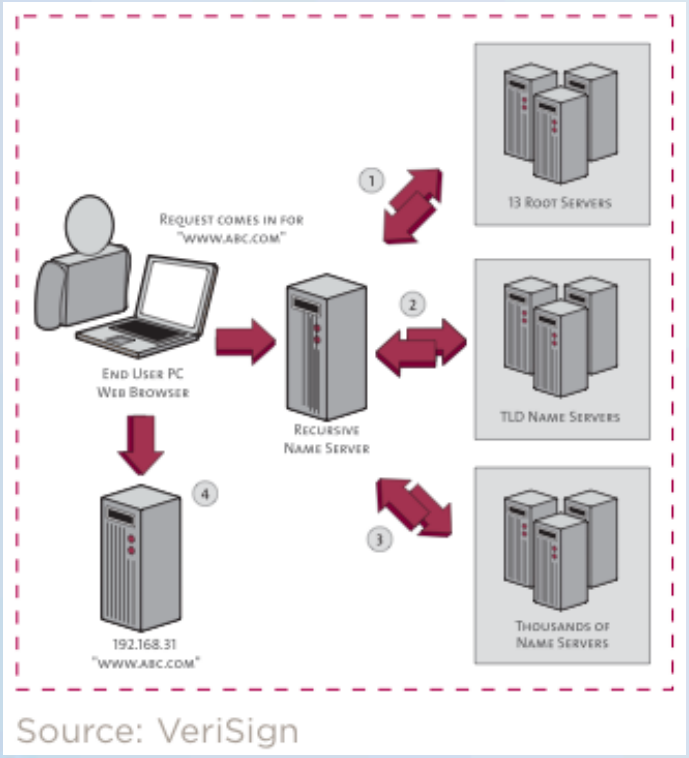
Registro de dominios bajo .cr

Agenda

- Introduction
- Process of DNSSEC.
- Evident costs.
- Not so evident costs.
- Conclusion.

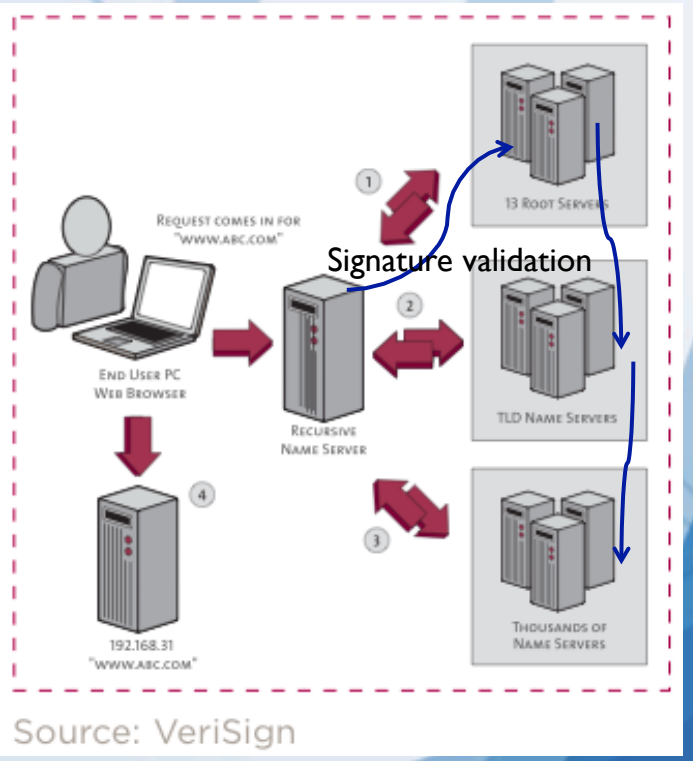
Introduction

DNS



Source: VeriSign

DNS+DNSSEC



Source: VeriSign

Introduction

CustomerPortal

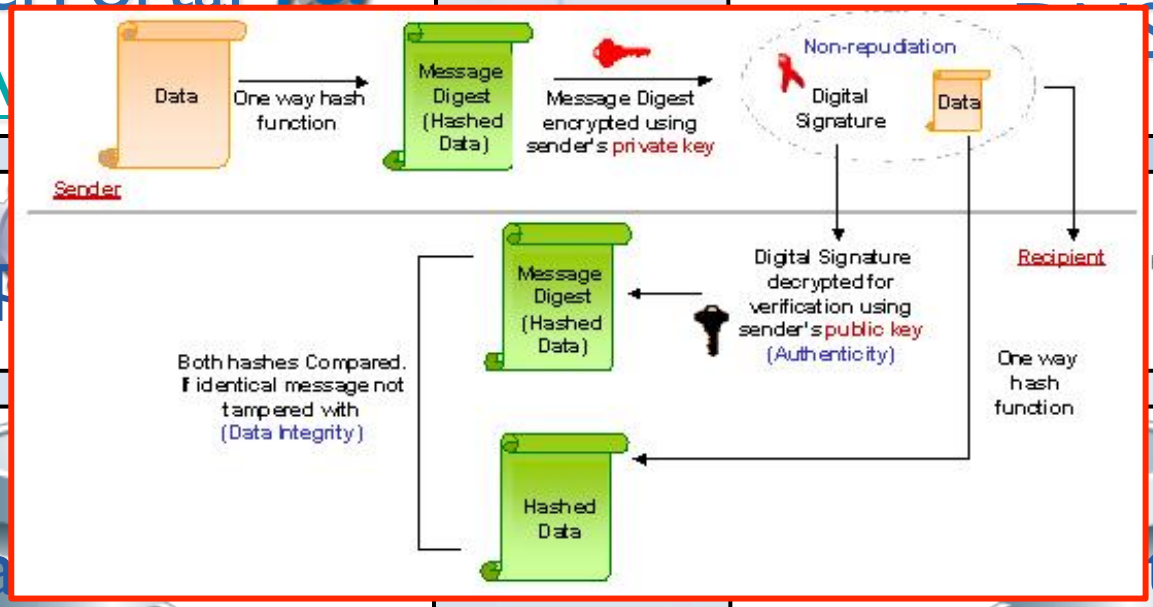
http://v

Web Ap

Da

tabase

ENUM AND DOMAINS



Automated Process

Our (small ccTLD) Concern about costs

- DNSSEC = DNS + Digital Signature
- DNS = Public Service on behalf of Internet
- Digital Signature for Public Service =Trust Certified.
- Trust Certified = Follow Security Standards
- Follow Security Standards = High cost in processes

Process of DNSSEC

RFC 4641

- Keeping the Chain of Trust Intact
- Keys Generation and Storage
- Signature Generation and Storage
- Key Rollover
- Policies

Evident costs

- Related directly with the size of zone:
  - Bandwidth: Increase 3 or 4 times.
  - CPU of servers: increase up to 50%.
  - Memory of servers: up to 4 times.
- Key generation hardware: SC or HSM
- Software changes.

Costs

- Bandwidth: Low impact
  - Costs of bandwidth decrease constantly.
  - Very low consumption compared with other Internet protocols.
- CPU and Memory of servers: Low impact
  - Typically over sized for DNS.
  - With DNSSEC the servers will start to use the CPU

Costs

- Key generation and storage: Predictable cost.
  - Smart Card: less than $100
  - HSM: $800 - $25000
- Software changes: Predictable cost.
  - Just add one field

Not so evident costs

- IT Staff time (research, setup and operations).
- Hardware and software maintenance.
- Changing and increasing operational procedures (maybe underestimate).
  - Key generation and store, signing, key rollover, key ceremony, etc.
- Definition of new policies.

Hidden costs

- IT Staff time: High cost.
  - New operations: Generation of keys, signatures of zones, key rollover, upload DS, automation of process. Need many hours of expensive resources (IT Staff).
- Hardware and software life cycle maintenance. (Est. 20% annual of initial cost)

Hidden costs

- Operational procedures: Very high
  - Similar to a Certificate Authority, more than 50% of costs are procedures.
  - Standardization involves the documentation of procedures.
  - Security Trust require documented and maintained procedures.

Hidden costs

- Key ceremony: (2 times a year, costs ?)
  - Initially for root-servers, but NIC.BR is doing now.
  - Key ceremony is not mentioned in RFC 4641, but is used in Certificate Authority.
- Policy: High Costs (Lawyers)
  - High responsibility because signature of the zones and the Registry adopt to role of public notary.

Conclusions

- The real costs of implement DNSSEC is indeterminable or hard to estimate for a small ccTLD and is higher than only acquire technology.
- The real high costs is mainly related the new procedures to keeping the chain of trust intact and less in technology.
- The benefit of implement DNSSEC is evident and necessary and justifies its cost.

Conclusions

- The chain is broken at the weakest link!
- In some future phase “somebody” must accredit the signing process of the links of the chain.

Questions?