



DNSSEC

Como implementarlo

Luciano Minuchin
luciano@arconsit.com

DNSSEC

Por que usar DNSSEC?

DNSSEC

Problemas del DNS

- ✓ El protocolo DNS no permite validar el origen información de una respuesta, puede ser Atacado por los diferentes tipos de ataques de *poisoning*
- ✓ Los Slaves no pueden validar si el Master con el que se comunican es el verdadero
- ✓ Los datos que se trasmiten en el DNS pueden ser Falsificados “*spoofed*” entre las distintas capas

DNSSEC

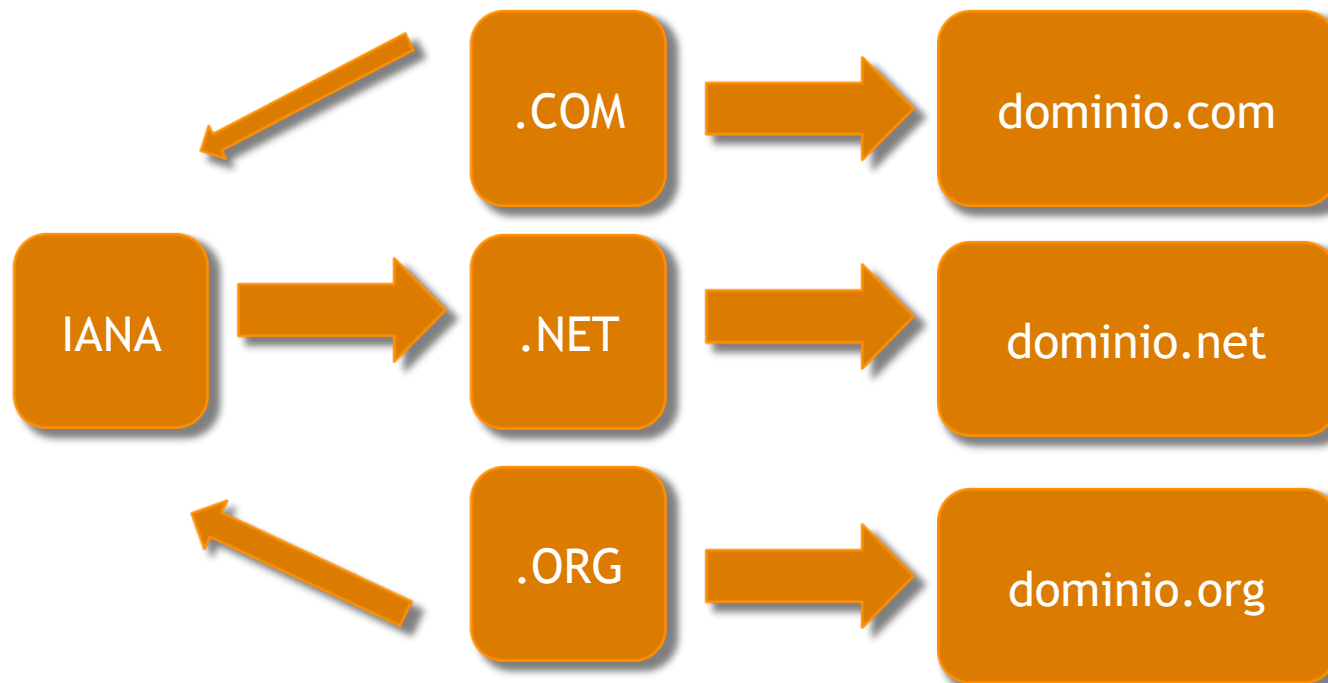
Es para todos?

- + Educación
- + Bancos
- + Seguros
- + Comercio Electrónico
- + Sitios de información relevante
- + Gobiernos Nacionales y Regionales
- + ISPs
- + Proveedores de Contenido
- + Hosting

DNSSEC

Cadenas de confianza (Trust Anchor)

Los niveles se firman con claves de la siguiente jerarquía



DNSSEC

BBB

Bueno, Bonito y Barato

DNSSEC

Que Necesito?

- ✓ Equipos que realizara la firma (PC con TPM o Smart Card)
- ✓ 6 Pen Drives
- ✓ Caja fuerte (pequeña)
- ✓ Bolsas de Evidencia o Valores
- ✓ 4 personas
- ✓ Su registrador de dominios tiene que permitir subir registros DS

DNSSEC

Primeros Pasos

- ✓ DPS (DNSSEC Practice Statement) Declaración de Políticas y Procedimientos
- ✓ Guion para la ceremonia de firmado
- ✓ Instalar un Linux + Bind en la PC

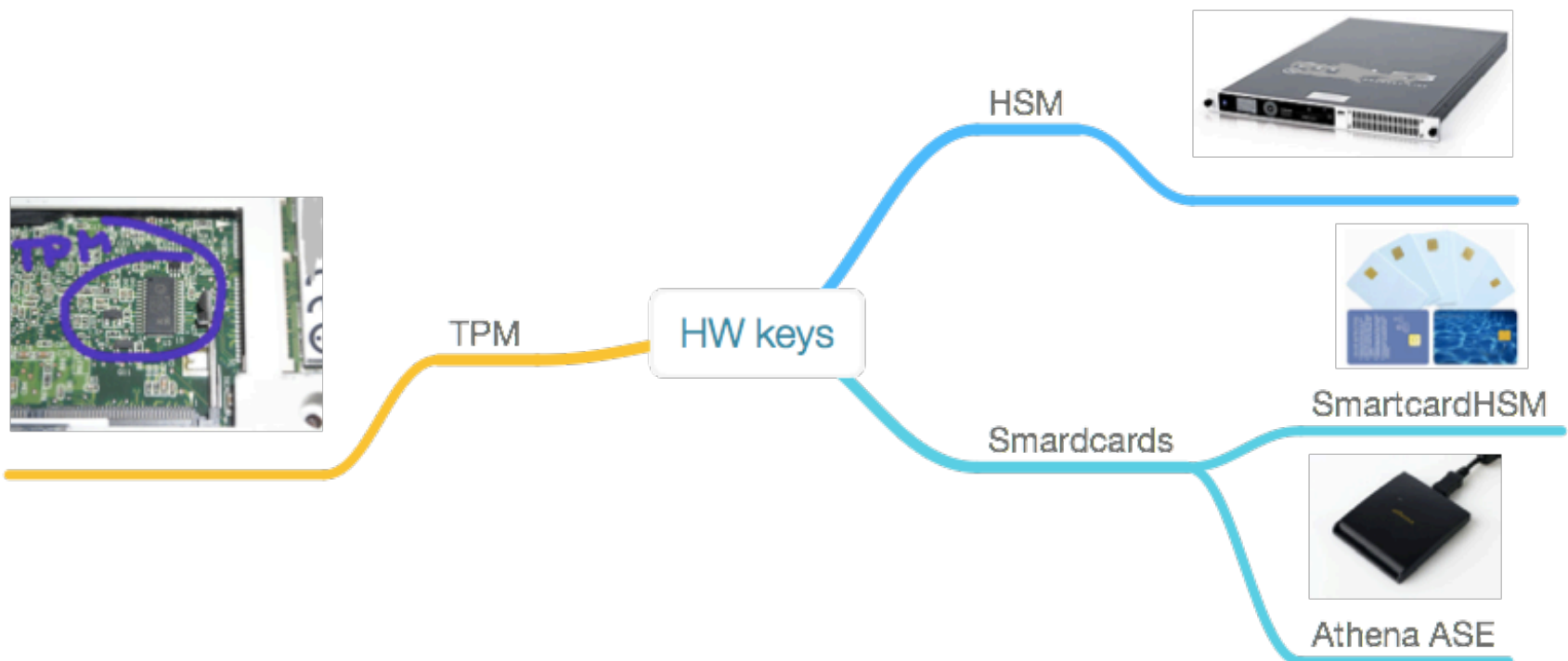
DNSSEC

Generación de llaves y Firma Inicial

- ① KSK
- ② ZSK
- ③ Firma la ZONA
- ④ Extraen la RRSIG
- ⑤ Se importan la llave ZSK + RRSIG en el server de DNS

DNSSEC

Generación de Llaves por Hardware



DNSSEC

Publicación de una Zona con DNSSEC

- ① Base de Datos
- ② Formato de archivo de Zona
- ③ Importa en el Linux+Bind -----> Firma Zona
- ④ Update del Serial
- ⑤ Reload de la zona

DNSSEC

LINKs IMPORTANTES

- <https://labs.nic.cz/en/projects.html>
- http://www.niclabs.cl/research_nic.html
- <http://www.nlnetlabs.nl>
- <https://www.iana.org/dnssec/ceremonies/24>
- <http://ri.co.cr/#schsm>

DNSSEC

<http://dnssec-debugger.verisignlabs.com>

<http://dnsviz.net>



Domain Name:

Analyzing DNSSEC problems for dnsviz.net

	- Found 3 DNSKEY records for . - DS=19030/SHA-1 verifies DNSKEY=19030/SEP - Found 1 RRSIGs over DNSKEY RRset - RRSIG=19030 and DNSKEY=19030/SEP verifies the DNSKEY RRset
net	- Found 1 DS records for net in the . zone - Found 1 RRSIGs over DS RRset - RRSIG=60615 and DNSKEY=60615 verifies the DS RRset - Found 2 DNSKEY records for net - DS=35886/SHA-256 verifies DNSKEY=35886/SEP - Found 1 RRSIGs over DNSKEY RRset - RRSIG=35886 and DNSKEY=35886/SEP verifies the DNSKEY RRset
dnsviz.net	- Found 2 DS records for dnsviz.net in the net zone - Found 1 RRSIGs over DS RRset - RRSIG=51128 and DNSKEY=51128 verifies the DS RRset - Found 2 DNSKEY records for dnsviz.net - DS=28345/SHA-1 verifies DNSKEY=28345/SEP - Found 1 RRSIGs over DNSKEY RRset - RRSIG=28345 and DNSKEY=28345/SEP verifies the DNSKEY RRset - dnsviz.net A RR has value 72.13.58.70 - Found 1 RRSIGs over A RRset - RRSIG=62748 and DNSKEY=62748 verifies the A RRset

Move your mouse over any or symbols for remediation hints.

Want a second opinion? Test dnsviz.net at dnsviz.net.



dnsviz.net

Updated: 2016-04-01 13:21:37 UTC (about 2 hours ago) [Update now](#)

[« Previous analysis](#) | [Next analysis »](#)

DNSSEC Responses Servers Analyze

— DNSSEC options ([show](#)) —

Notices

DNSSEC Authentication Chain

Download: [png](#) | [svg](#)

Mouse over and click eler

RRset status

Secure (4)

DNSKEY/DS/NSEC status

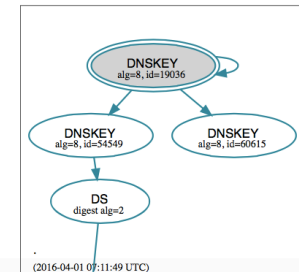
Secure (9)

Delegation status

Secure (2)

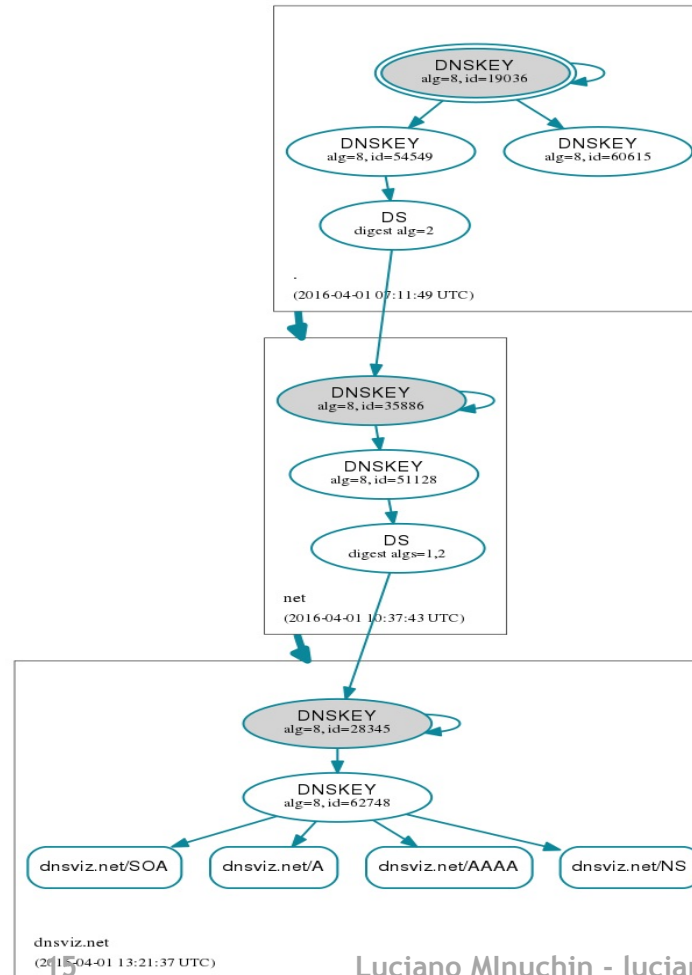
DNSKEY legend

Full legend
 SEP bit set
 Revoke bit set
 Trust anchor



DNSSEC

Cadena de Confianza



DNSSEC

GRACIAS!!!

Consultas y Ayuda

luciano@arconsit.com