

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas



To Sec or Not To Sec – DNS Question



○ Raúl Siles



monica@dinosec.com ○

○ raul@dinosec.com

○ Mónica Salas





2018

DINSSEC

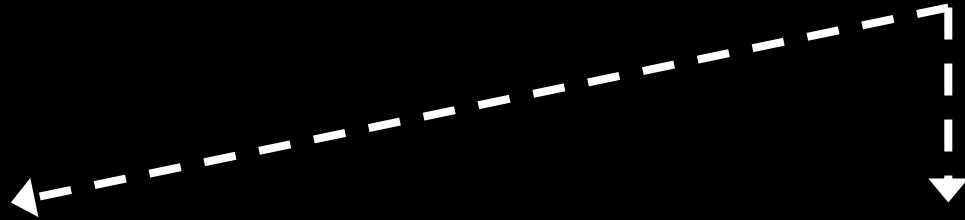


https://

**¿Quién está haciendo uso de
DNSSEC?**

Firmado de zona

Validación

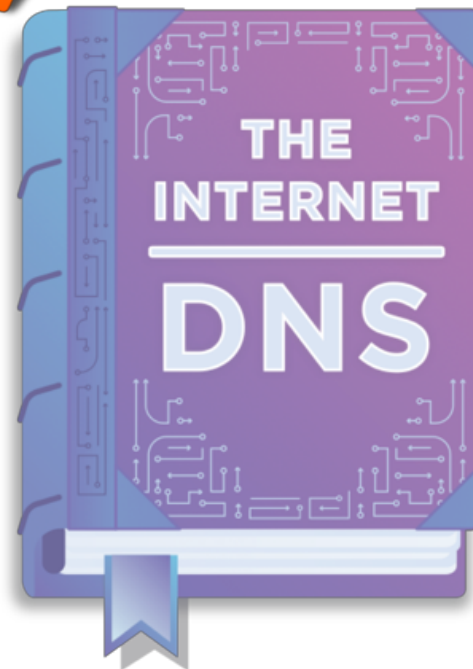




Índice



- DNSSEC - ¿Por qué y qué?
- Arquitectura de DNSSEC
 - Firmado de zona en DNSSEC
 - Resolución de nombres y validación en DNSSEC
- Estado de implantación de DNSSEC
- Argumentos **desfavorables** para la implantación de DNSSEC
- Argumentos **favorables** para la implantación de DNSSEC
- *Despliegue de DNSSEC completado: Y ahora...*
- Conclusiones
- Referencias

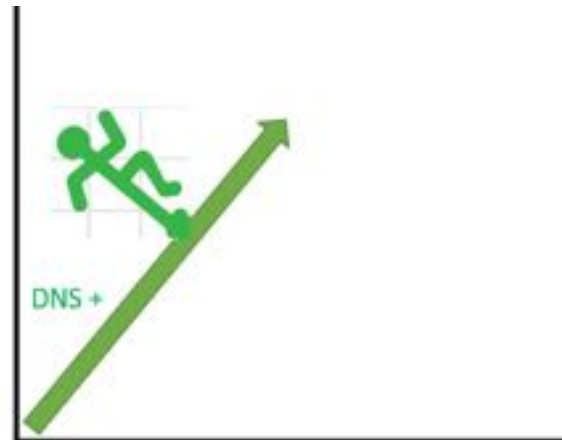
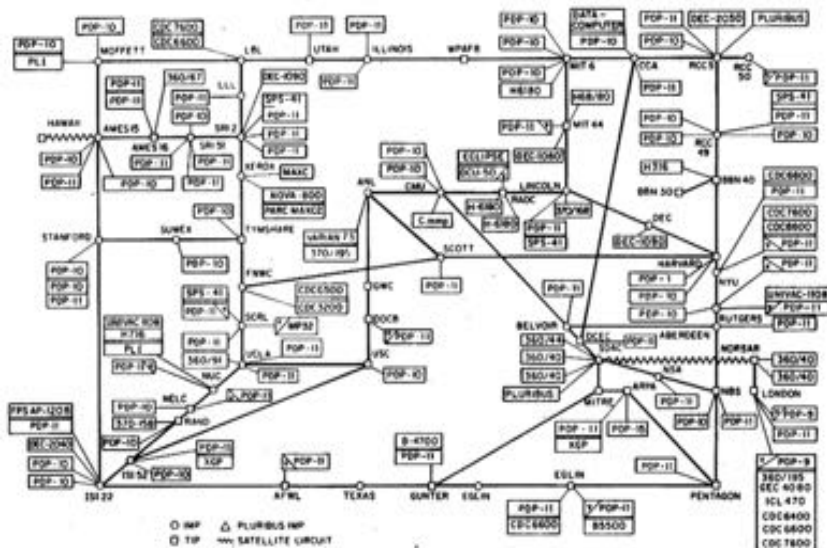




DNSSEC- ¿Por qué y qué?

Sin DNS no existiría la Internet de hoy en día...

ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE MOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES



DNSSEC - ¿Por qué y qué? (1/2)

¿Por qué DNSSEC?

- DNS adolece, por diseño, de múltiples problemas de seguridad...
 - Permite suplantación de identidad (ataques MitM)
 - Permite alteración de los datos (ataques de envenenamiento de caché)

DNS cache poisoning

DNS spoofing



Servidor DNS

El 76% de las organizaciones participantes en el estudio de Efficient IP(*) sufrieron ataques de DNS durante 2017, con robo de datos en un 28% de ellos. El 23% fueron envenenamientos de caché.

(*) http://www.efficientip.com/wp-content/uploads/PR_DNS_Threat_Survey_2017.pdf

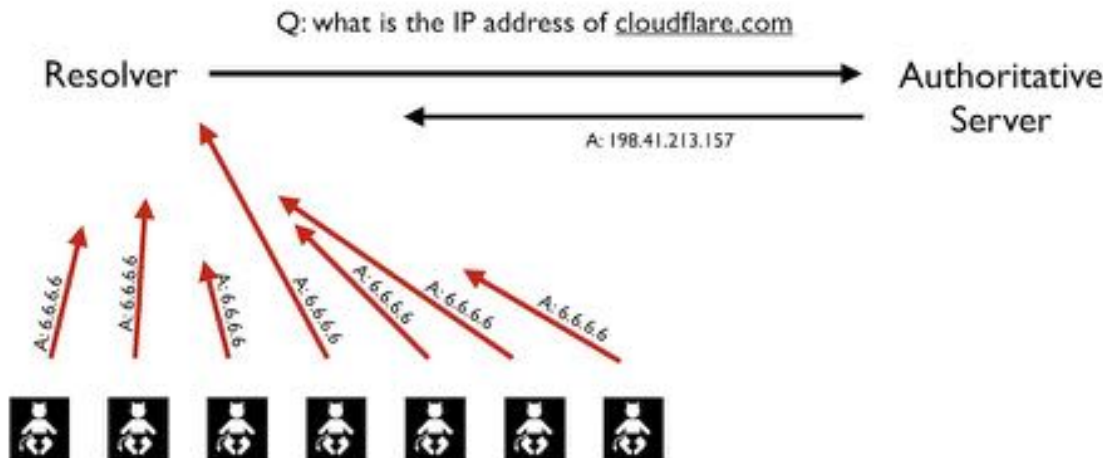


Ataques sobre DNS

- Suplantación de DNS (MitM): ARP, BGP, aLTER, etc.



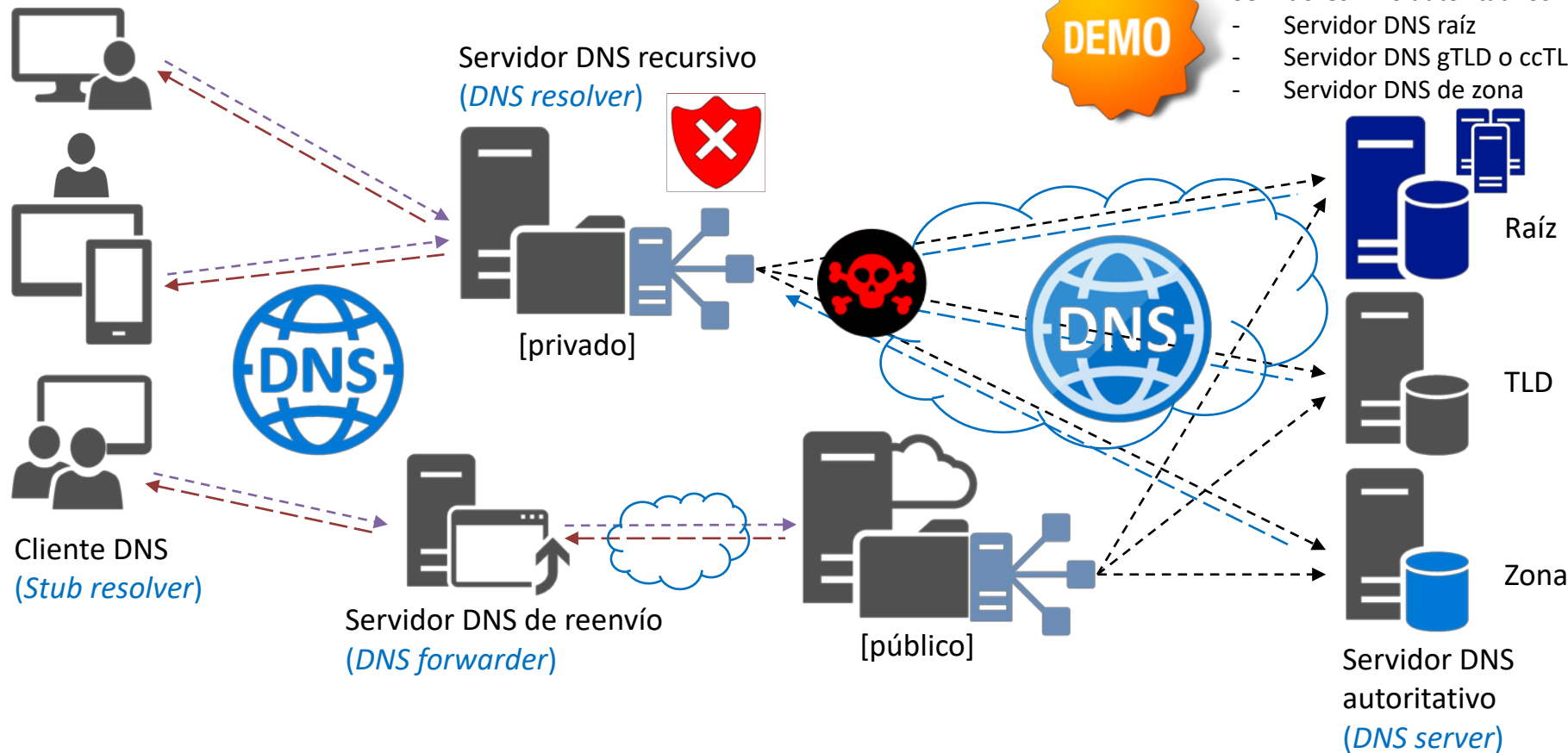
- Envenenamiento de caché DNS (Kaminsky)

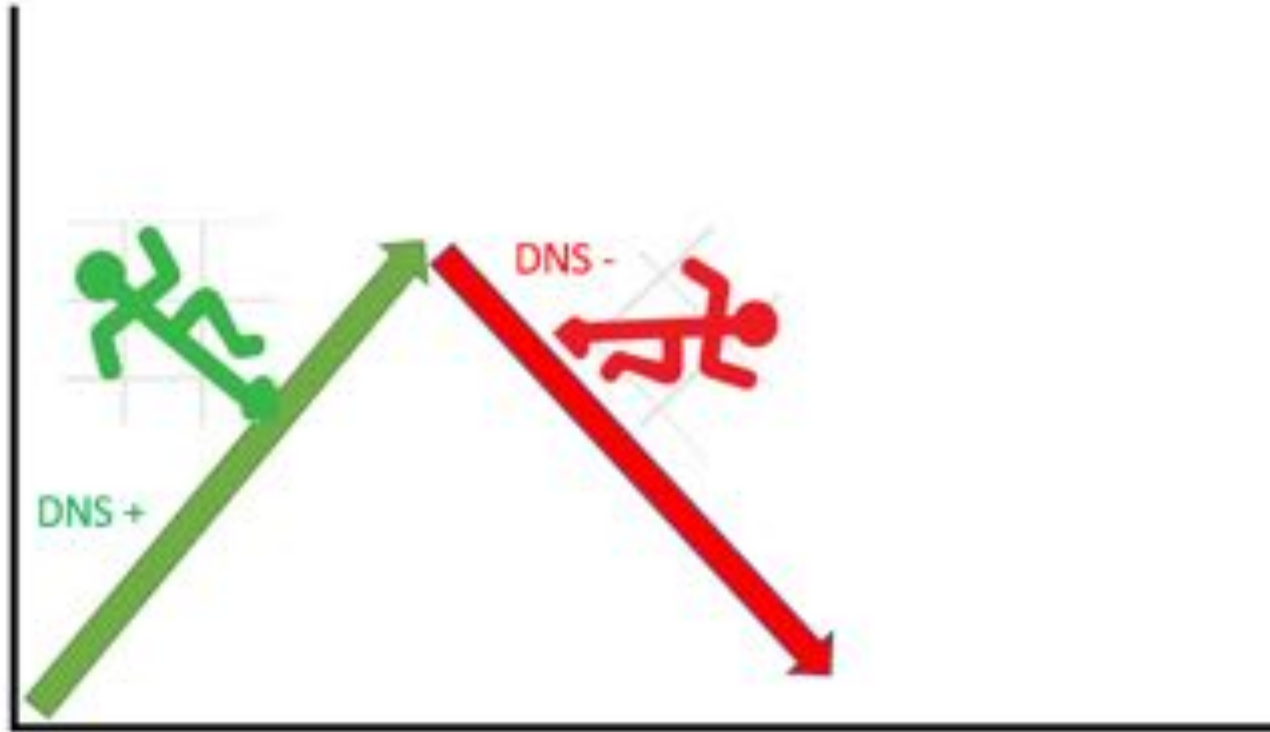




Servidores DNS autoritativos:

- Servidor DNS raíz
- Servidor DNS gTLD o ccTLD
- Servidor DNS de zona







DNSSEC - ¿Por qué y qué? (2/2)

¿Qué es DNSSEC?

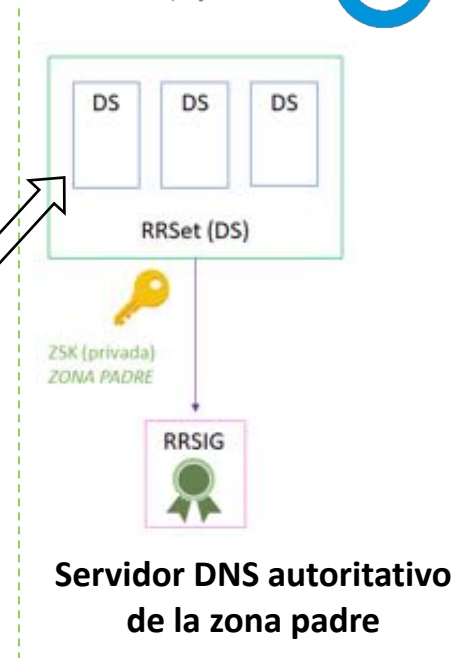
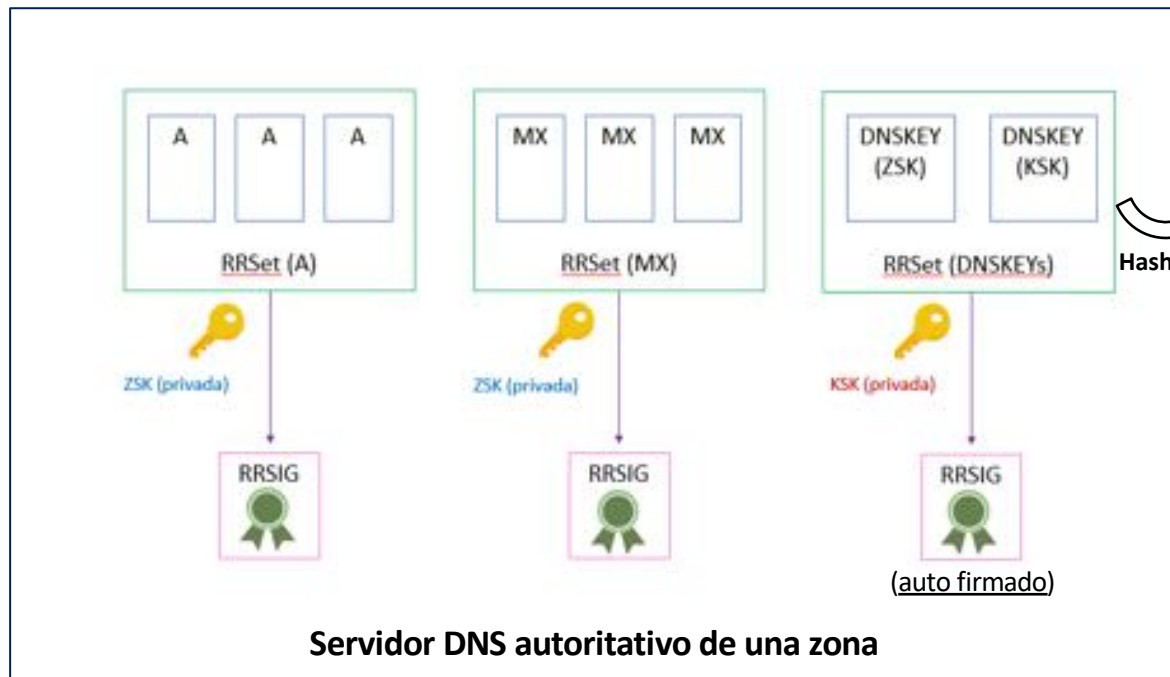
- Extensiones de seguridad del protocolo DNS para proporcionar mecanismos de verificación de:
 - Integridad de la respuesta → no ha sido alterada desde el origen
 - Autenticidad de la respuesta → procede del servidor legítimo
 - Autenticidad de respuestas negativas → recursos inexistentes en la zona
- Firma digital mediante un esquema de clave pública (PKI):
 - En todos los niveles de la jerarquía DNS
 - Cadena de confianza desde la zona raíz (root) → anclaje de confianza
 - Se firman los recursos de la zona y se incorporan estas firmas como un registro más de la respuesta DNS



Arquitectura de DNSSEC

Arquitectura de DNSSEC

Firmado de zona



ZSK = Zone Signing Key
KSK = Key Signing Key
DS = Delegation Signer



Ejemplo de zona firmada con DNSSEC

[View on GitHub](#)

DNSviz is a tool for visualizing the status of a DNS zone. It was designed as a resource for understanding and troubleshooting deployment of the DNS Security Extensions (DNSSEC). It provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and it lists configuration errors detected by the tool. Your [feedback](#) is appreciated.

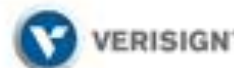
[Tweet](#) [G+](#)

Enter a domain name

Go

e.g., [www.example.com](#)

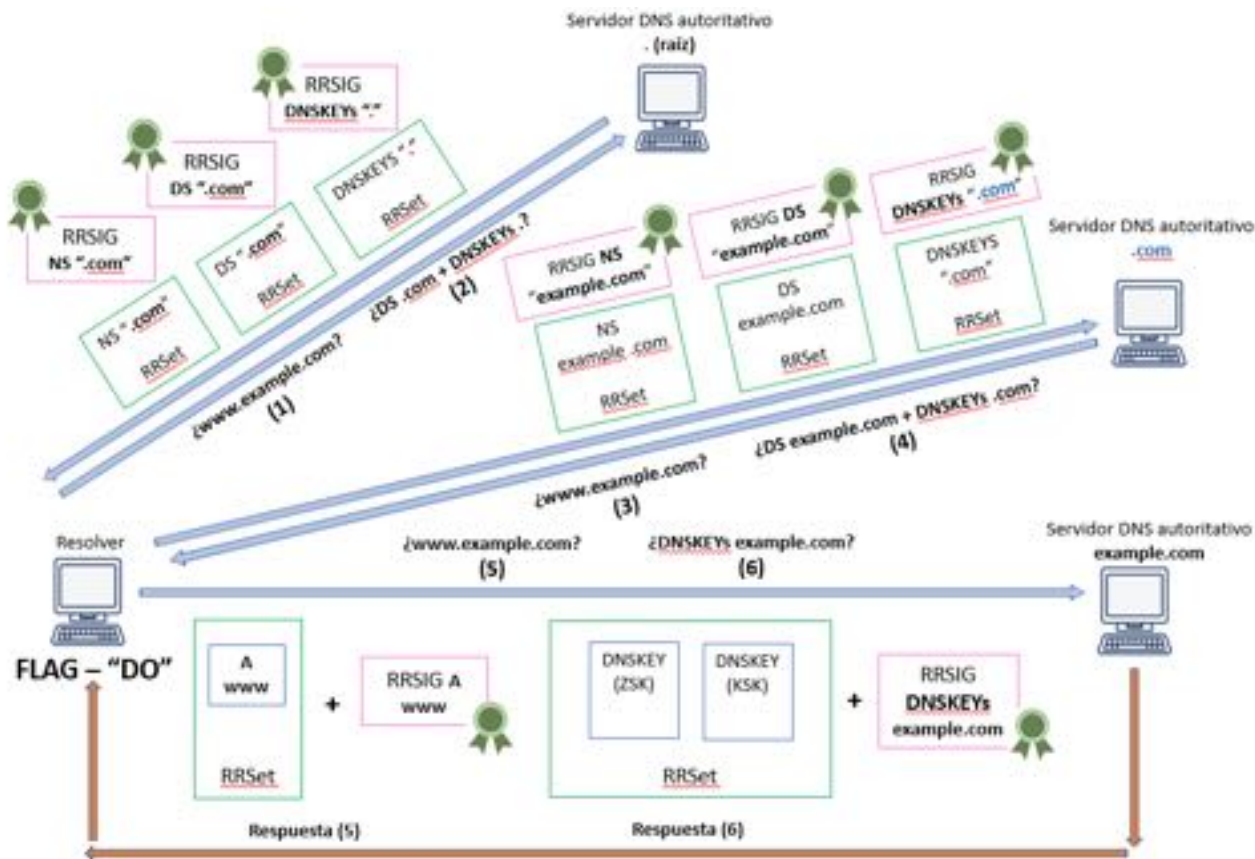
[Questions and Comments](#)



DEMO

DNSviz (<http://dnsviz.net>)

Proceso iterativo de resolución de nombres en DNSSEC

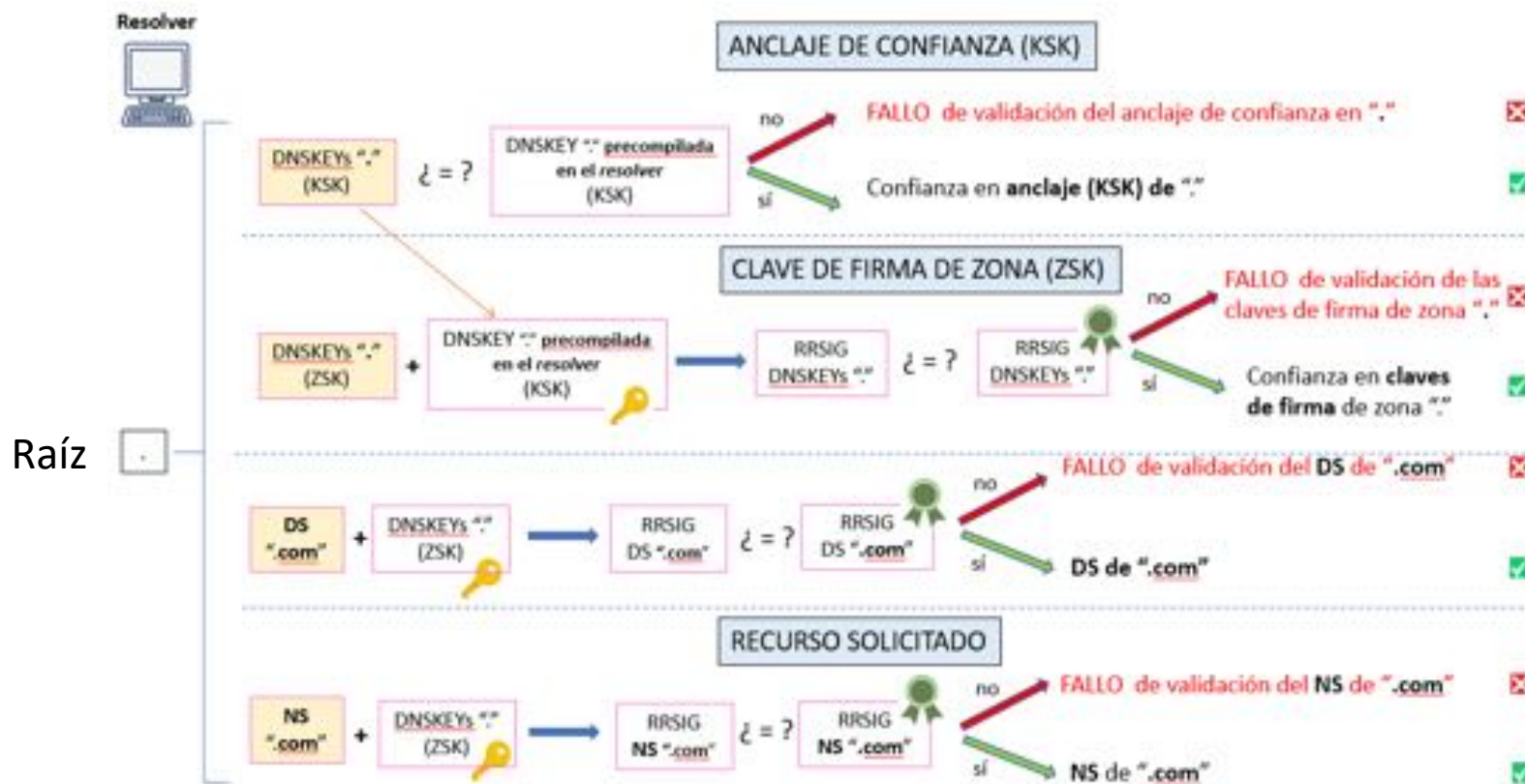




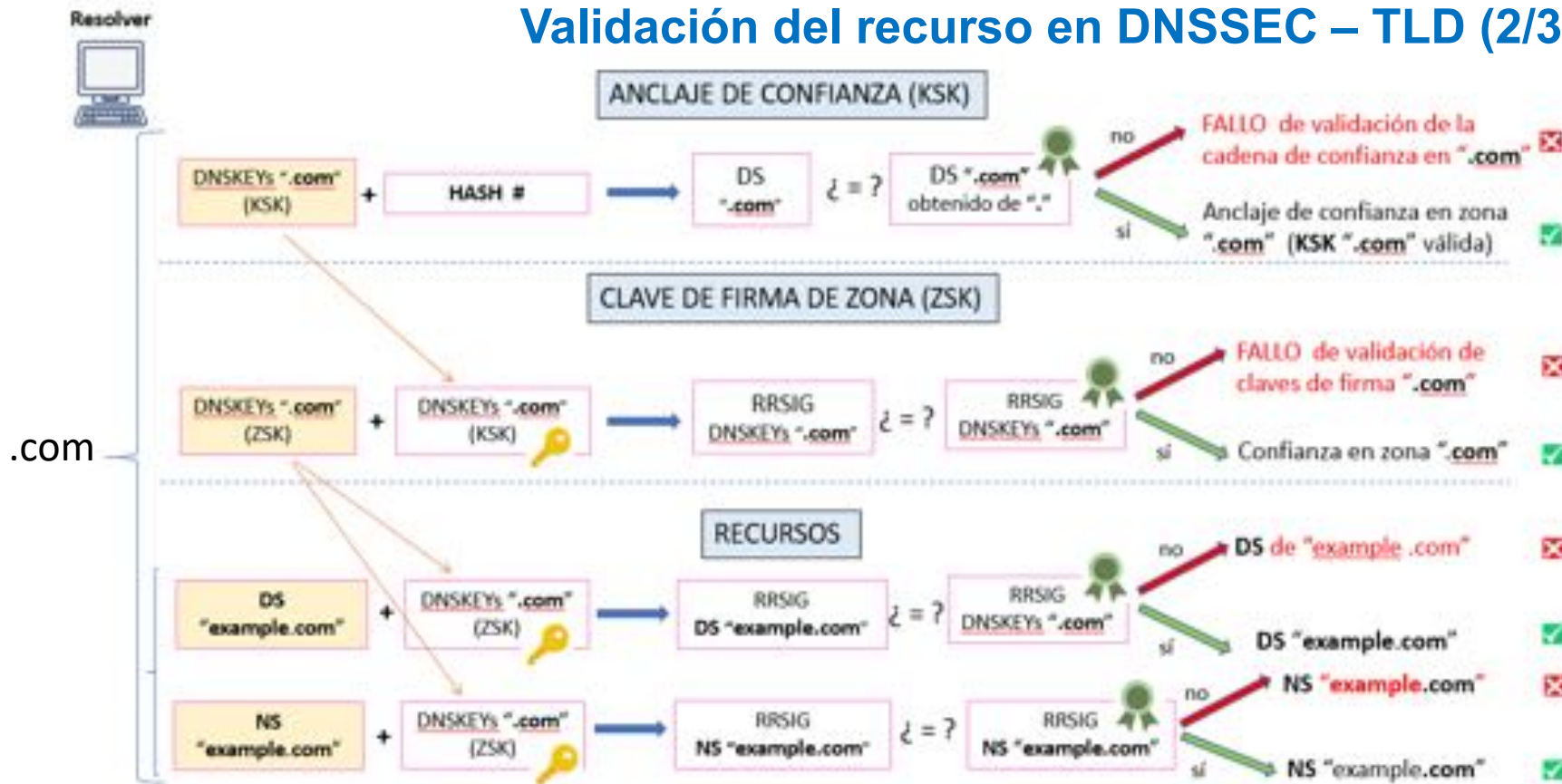
Validación de recursos mediante DNSSEC

- Anclaje de confianza (con la zona padre)
 - Autenticidad de la KSK → procede del servidor autoritativo de la zona
- Clave de firma de zona (ZSK)
 - Autenticidad de la ZSK → pertenece al servidor autoritativo de la zona
 - Integridad de los recursos servidos → garantía de la cadena de confianza
- Recurso DNS solicitado
 - Autenticidad del recurso → lo ha firmado el servidor autoritativo
 - Integridad del recurso → no ha sido alterado desde el origen

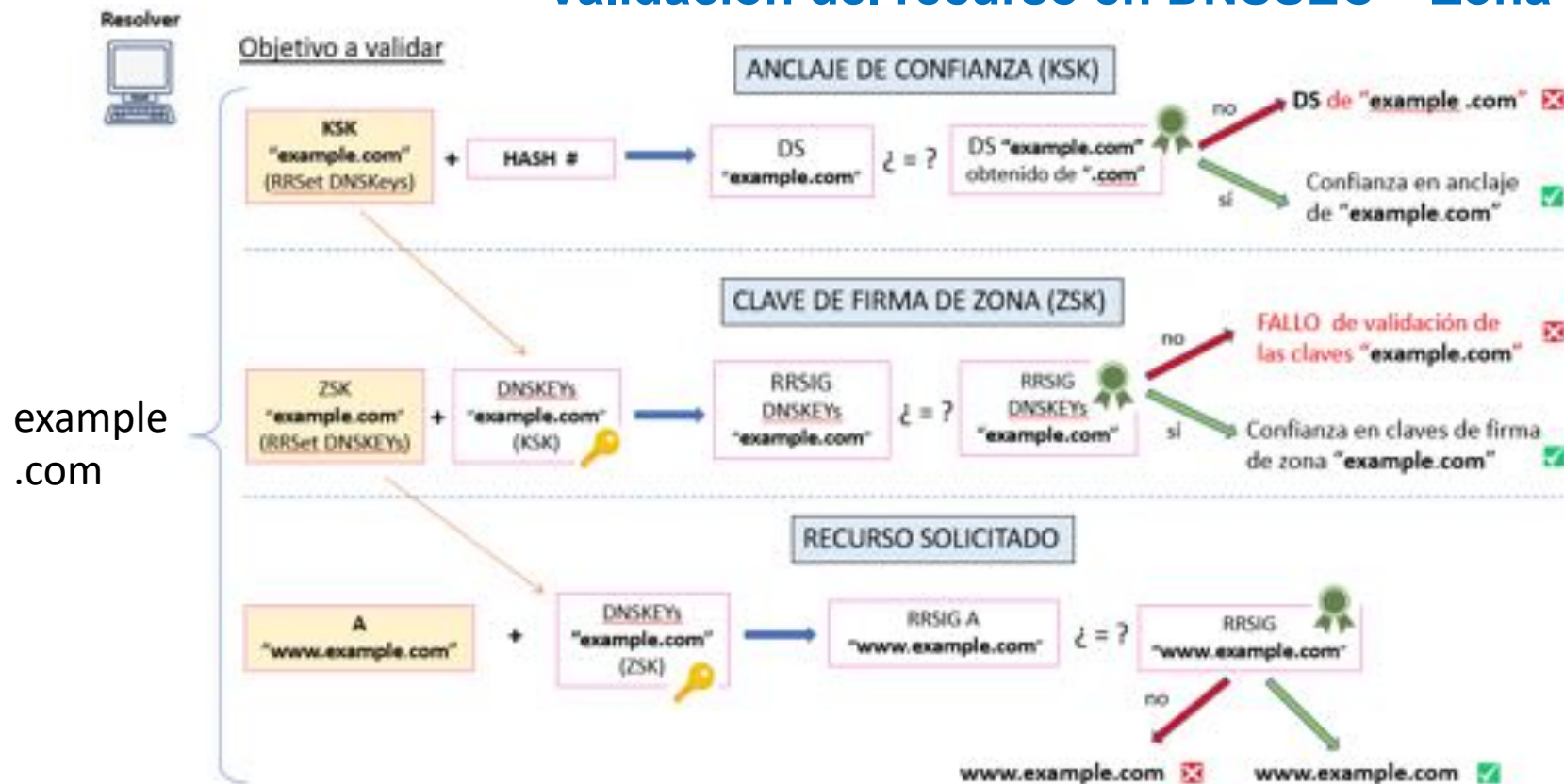
Validación del recurso en DNSSEC – Zona raíz (1/3)



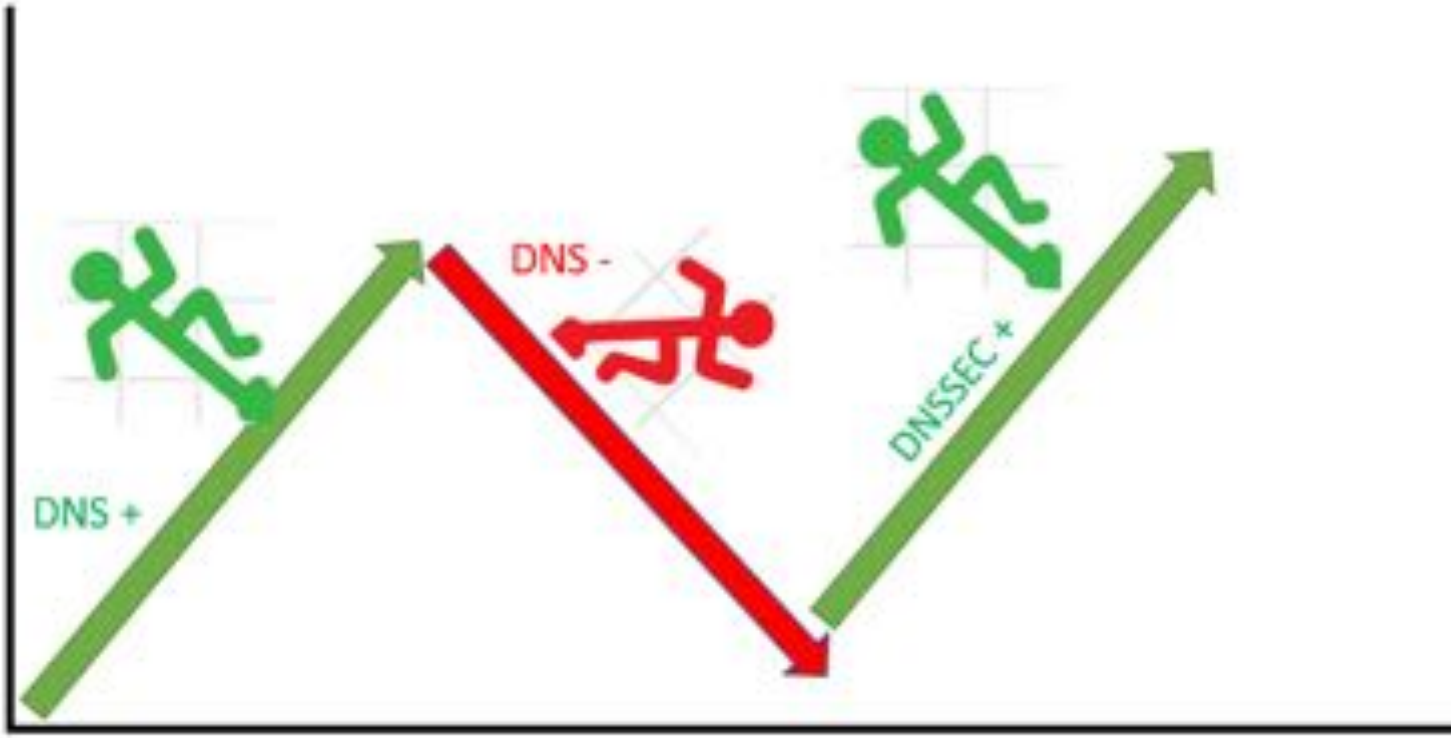
Validación del recurso en DNSSEC – TLD (2/3)



Validación del recurso en DNSSEC – Zona (3/3)



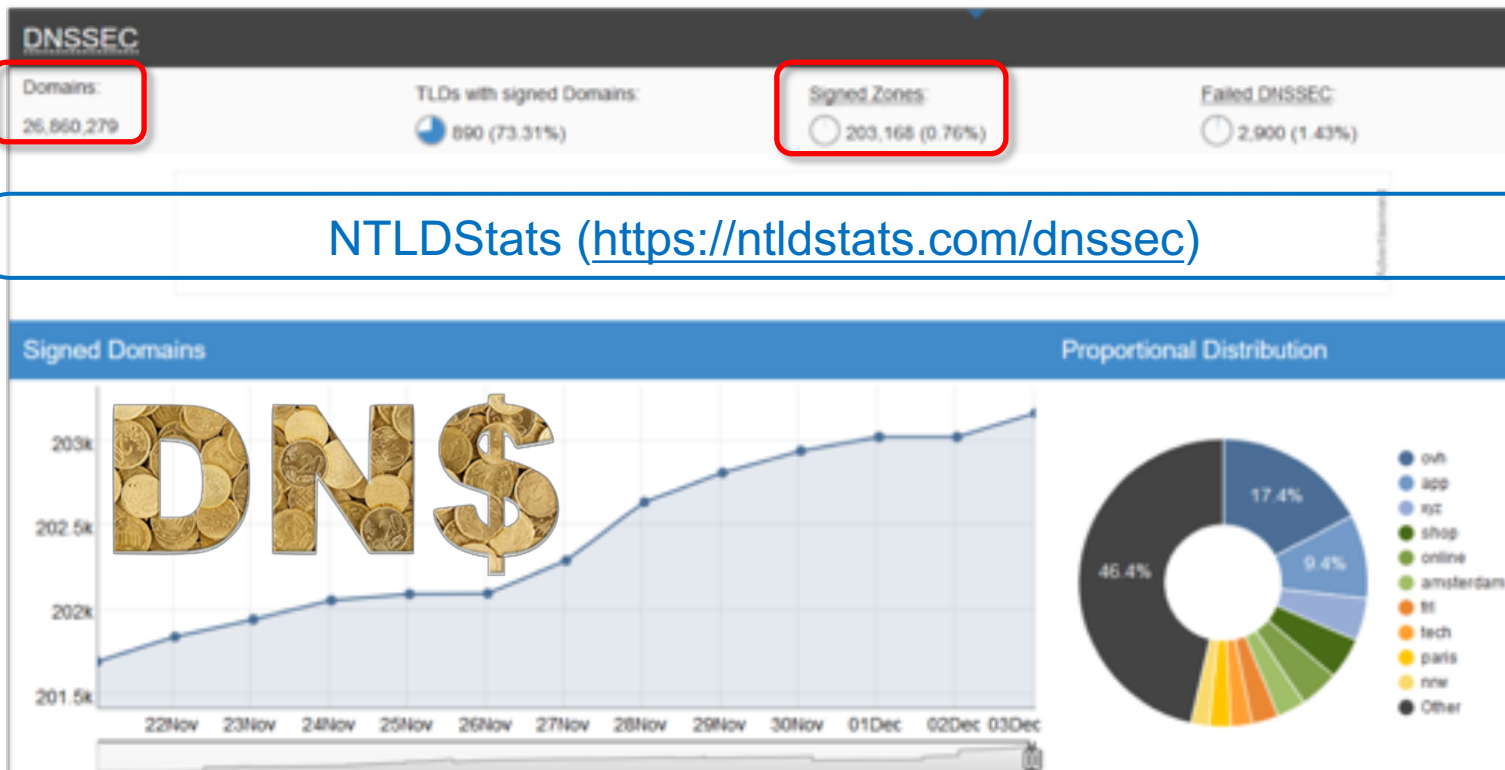






Estado de implantación de DNSSEC

Estado de implantación de DNSSEC



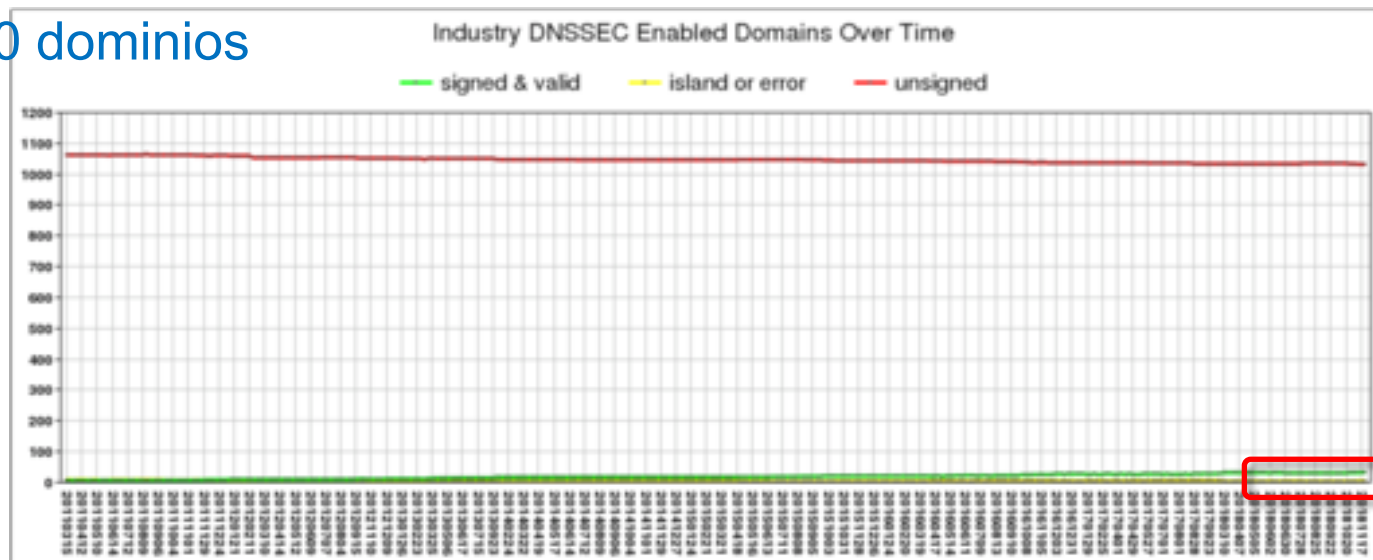
NTLDStats (<https://ntldstats.com/dnssec>)



Estado de implantación de DNSSEC en los dominios más relevantes

Fortune 1000 (NIST)

- **3%** de las empresas de Fortune 1000 firman sus dominios principales
- **Industria: 1.070 dominios**
 - .com
 - .net
 - .org



<https://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-com>

Estado de implantación de DNSSEC: ccTLDs (1/2)

ccTLD DNSSEC Status on 2018-12-03



EUR ccTLD DNSSEC Status on 2018-12-03



Fuente: Internet Society (<https://www.internetsociety.org/deploy360/dnssec/maps/>)

Estado de implantación de DNSSEC: ccTLDs (2/2)

NA ccTLD DNSSEC Status on 2017-12-03



LAC ccTLD DNSSEC Status on 2017-12-03

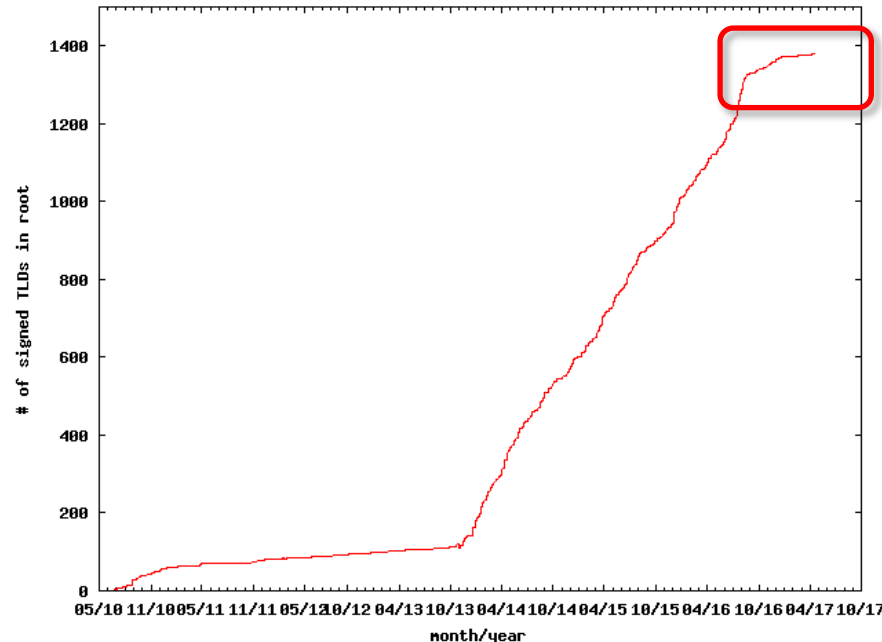


Fuente: Internet Society (<https://www.internetsociety.org/deploy360/dnssec/maps/>)

Estado de implantación de DNSSEC: TLDs (gTLDs y ccTLDs)

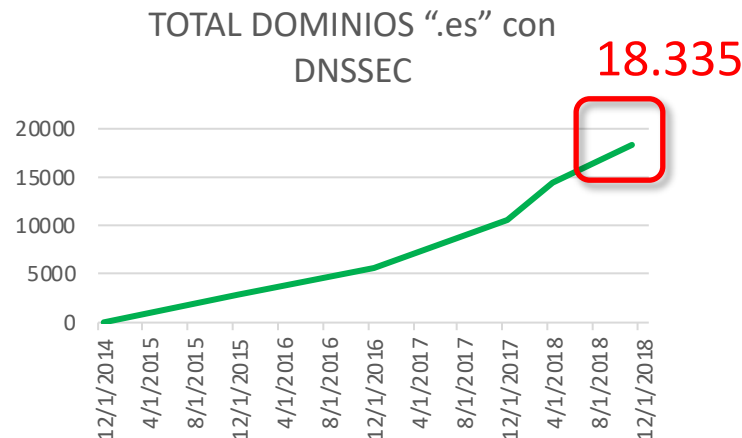
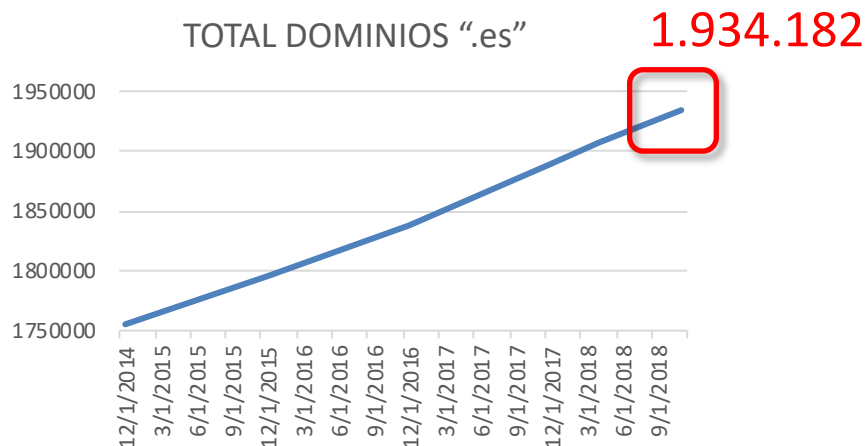
TLD DNSSEC Report (2018-12-03 00:02:23)

- **1535 TLDs** in the root zone in total
- **1400 TLDs signed (91%)**
 - Including .com, .org, .net, .edu... (gTLDs)
- 1391 TLDs have trust anchors published as DS records in the root zone
- 0 TLDs have trust anchors published in the ISC DLV Repository



Estado de implantación de DNSSEC en España (.es)

Evolución de TLDs de segundo nivel bajo “.es”



< 1% zonas firmadas en "es"

39 / 102 *registrars* ofrecen DNSSEC (38%)

Top 5 *registrars* (46%) → 2,3% DNSSEC

Top 5 DNSSEC *registrars* → 95% DNSSEC

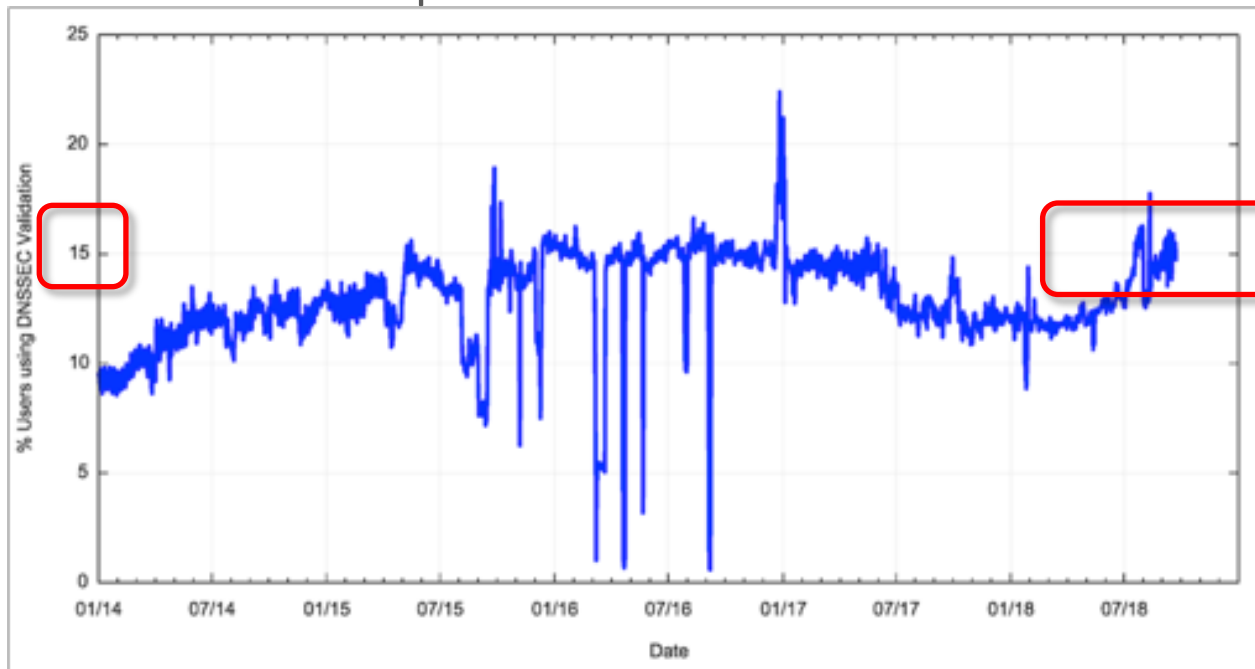


¿Cuál es entonces el interés actual en DNSSEC...?



Estado de implantación de la validación de DNSSEC

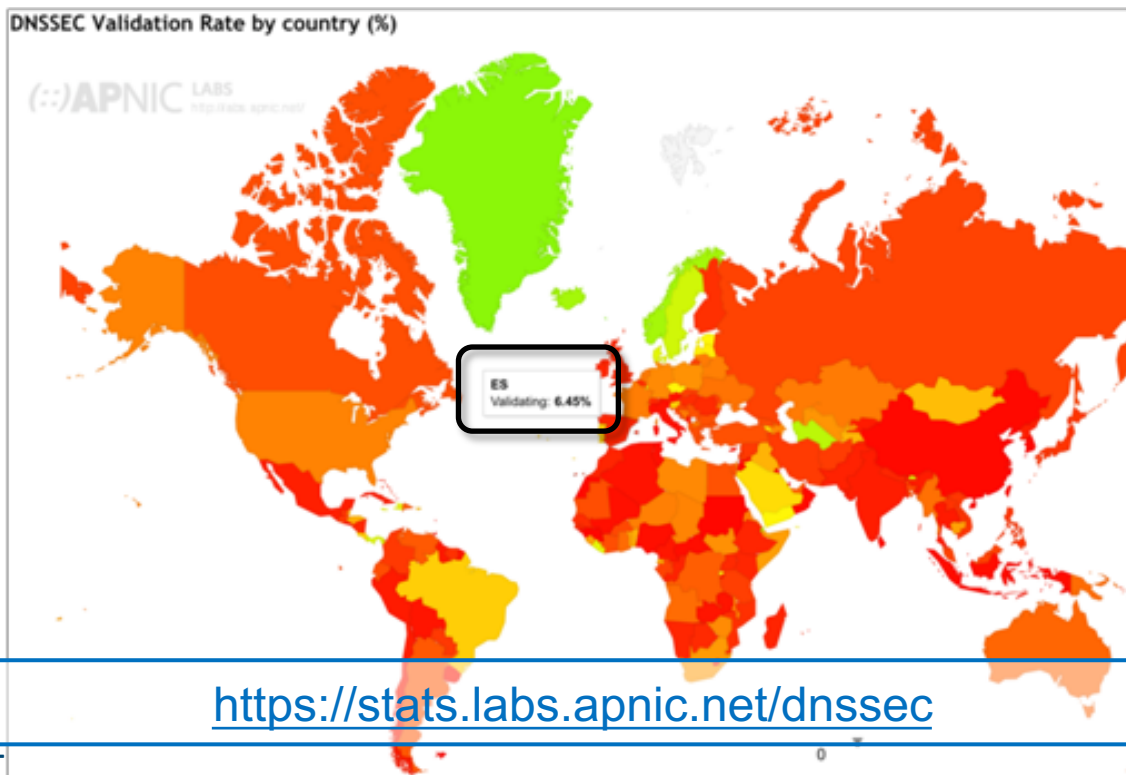
Usuarios con resolvers DNS que validan mediante DNSSEC: $\approx 15\%$



<https://blog.apnic.net/2018/09/28/measuring-the-ksk-roll/>

Estado de implantación de la validación de DNSSEC: España

Europa: 17,63% (<https://stats.labs.apnic.net/dnssec/XA>) – España: 6,5-9%





Argumentos **desfavorables** para la implantación de DNSSEC



Complejidad de DNSSEC

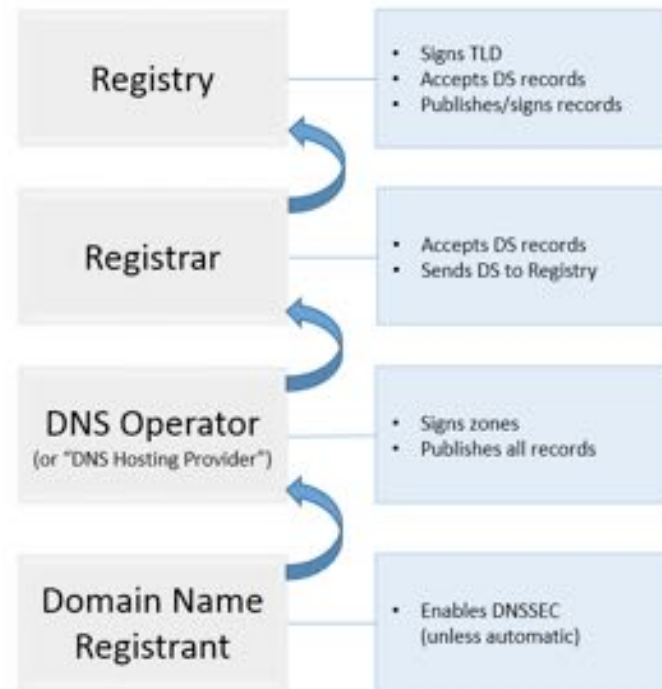
Actores

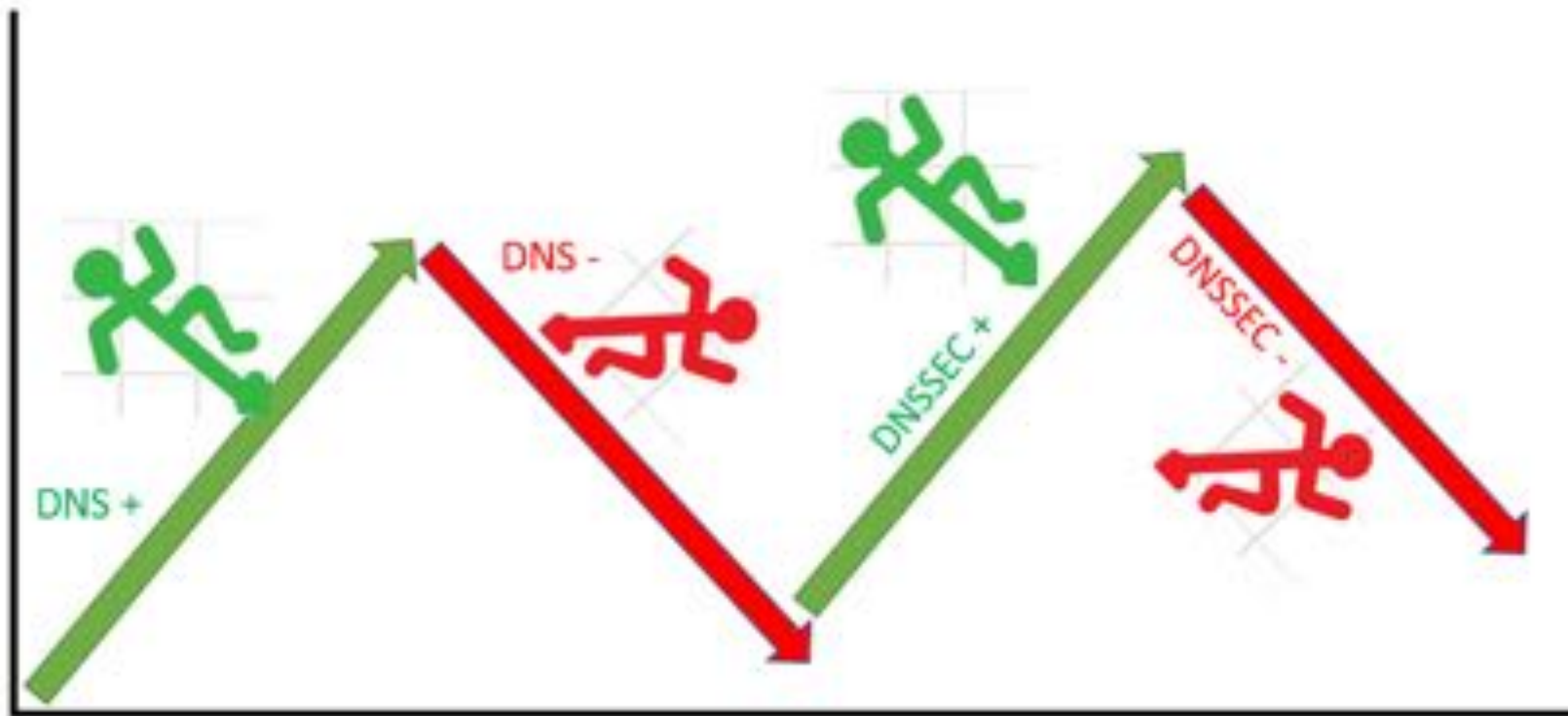
- Operador de DNS (propietario o tercero)
- CDNs y servicios DNS "en la nube"
- (Agente) Registrador
- Registro (TLDs)

Relaciones de confianza: registros DS

Complejidad técnica de DNSSEC

- Firmado de zona
- Gestión y renovación de claves
- Gestión y renovación de algoritmos criptográficos







Argumentos **favorables** para la implantación de DNSSEC



Simplificando DNSSEC (1/2)

- Actores
 - Gestión automática y sencilla, y/o por defecto, de la firma de la zona en (agentes) registradores (ej. ".es") y operadores de DNS (ej. Cloudflare)
 - Sin coste adicional
- Relaciones de confianza: registros CDS y CDNSKEY (Child ...)
 - RFC 8078: Managing DS Records from the Parent via CDS/CDNSKEY
 - <https://tools.ietf.org/html/rfc8078>
- Complejidad técnica de DNSSEC
 - DNS resolver recursivo
 - Servidor DNS autoritativo



Simplificando DNSSEC (2/2)

- DNS resolver recursivo
 - DNSSEC soportado en las implementaciones de resolvers recursivos
 - Habilitado con las opciones por defecto
 - Resolvers públicos reconocidos ofrecen soporte de DNSSEC
- Servidor DNS autoritativo
 - Variedad de software DNS de código abierto que casi automatiza la gestión del entorno: claves, firmado on-line de registros, renovación de *trust-anchor*...
 - Herramientas automáticas de gestión de código abierto
 - `dnssec-*` (Bind 9), OpenDNSSEC (www.opendnssec.org), Knot, PowerDNS...



Iniciativas para aumentar la adopción de DNSSEC

- SIDN (.nl)



- <https://www.sidn.nl/pages/registrar-overview.html>

- EU (.eu)



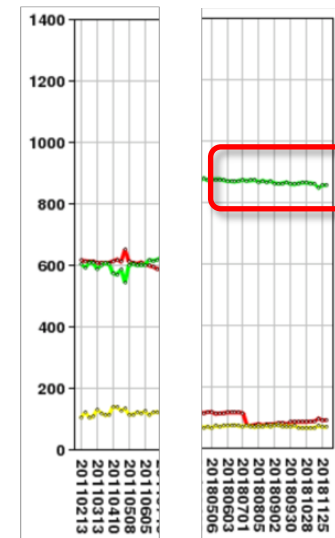
- <https://eurid.eu/en/find-a-registrar/>

- Obligatorio para los dominios .gov US – FISMA (≈80%)

- <https://rollready.dnsops.gov/FISMA-dnssec.html>
 - <https://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov>

- Incentivos económicos (para los distintos actores), ROI, posicionamiento de negocio...

- <https://blog.apnic.net/2018/04/24/bang-for-buck-the-adoption-of-dnssec-and-return-on-investment/>





**Imaginemos que ya os hemos
convencido y todos tenemos
implantado DNSSEC...**





PROBLEMÁTICA DE LA **ÚLTIMA MILLA**



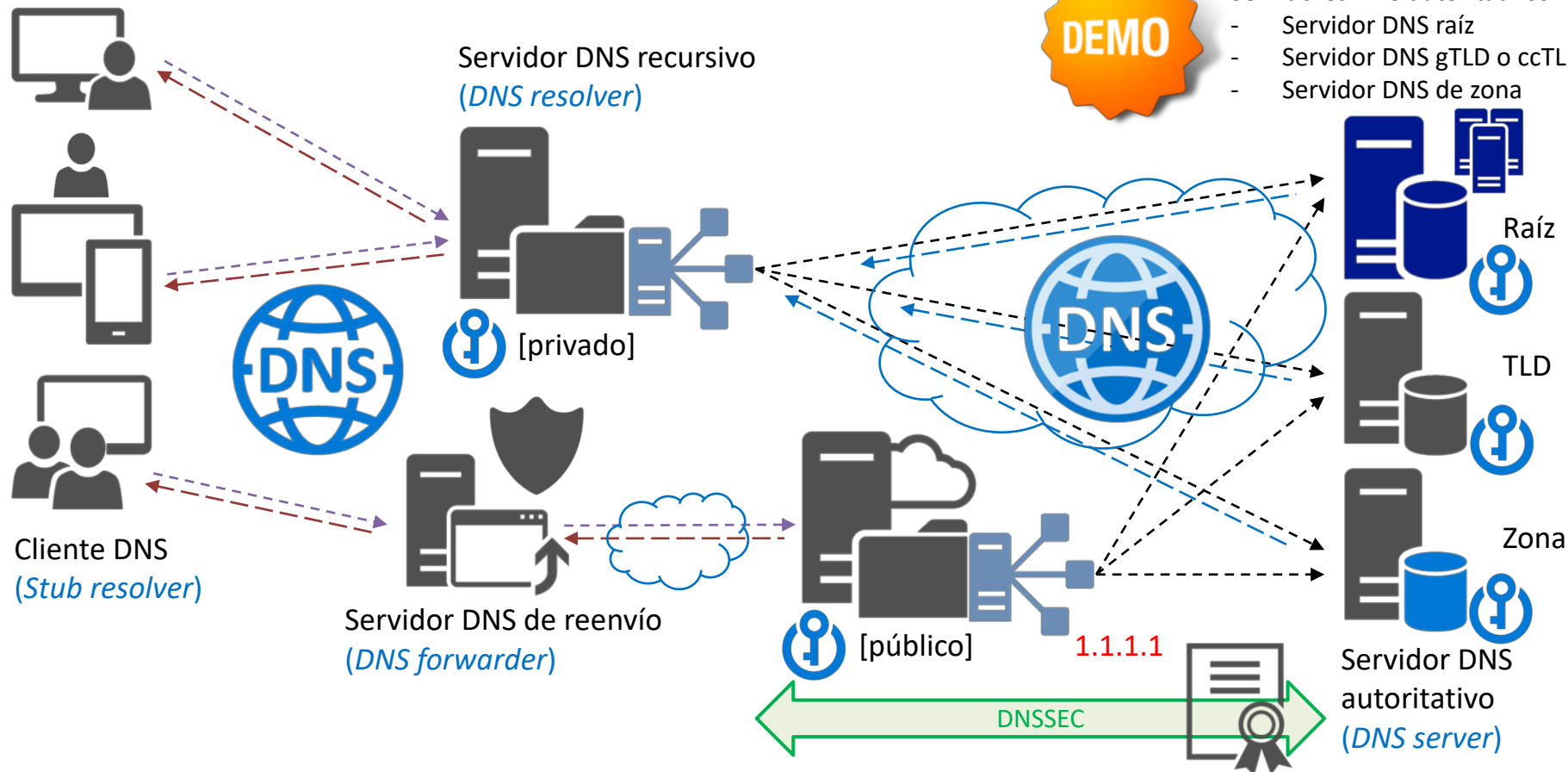
1 de abril de 2018





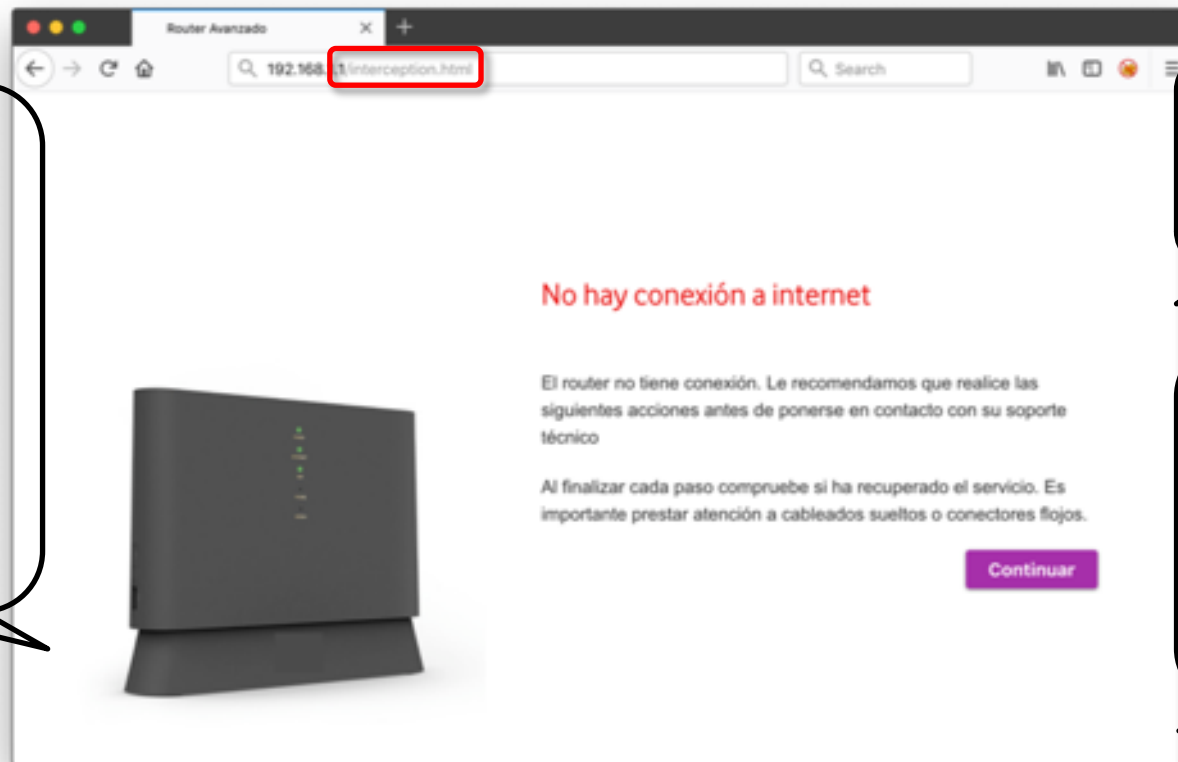
Servidores DNS autoritativos:

- Servidor DNS raíz
- Servidor DNS gTLD o ccTLD
- Servidor DNS de zona



Probando 1.1.1.1 (o one.one.one.one) con el resolver DNS local...

Por HTTP(S) muestra el interfaz web del router, pero resuelve bien todas las peticiones DNS...



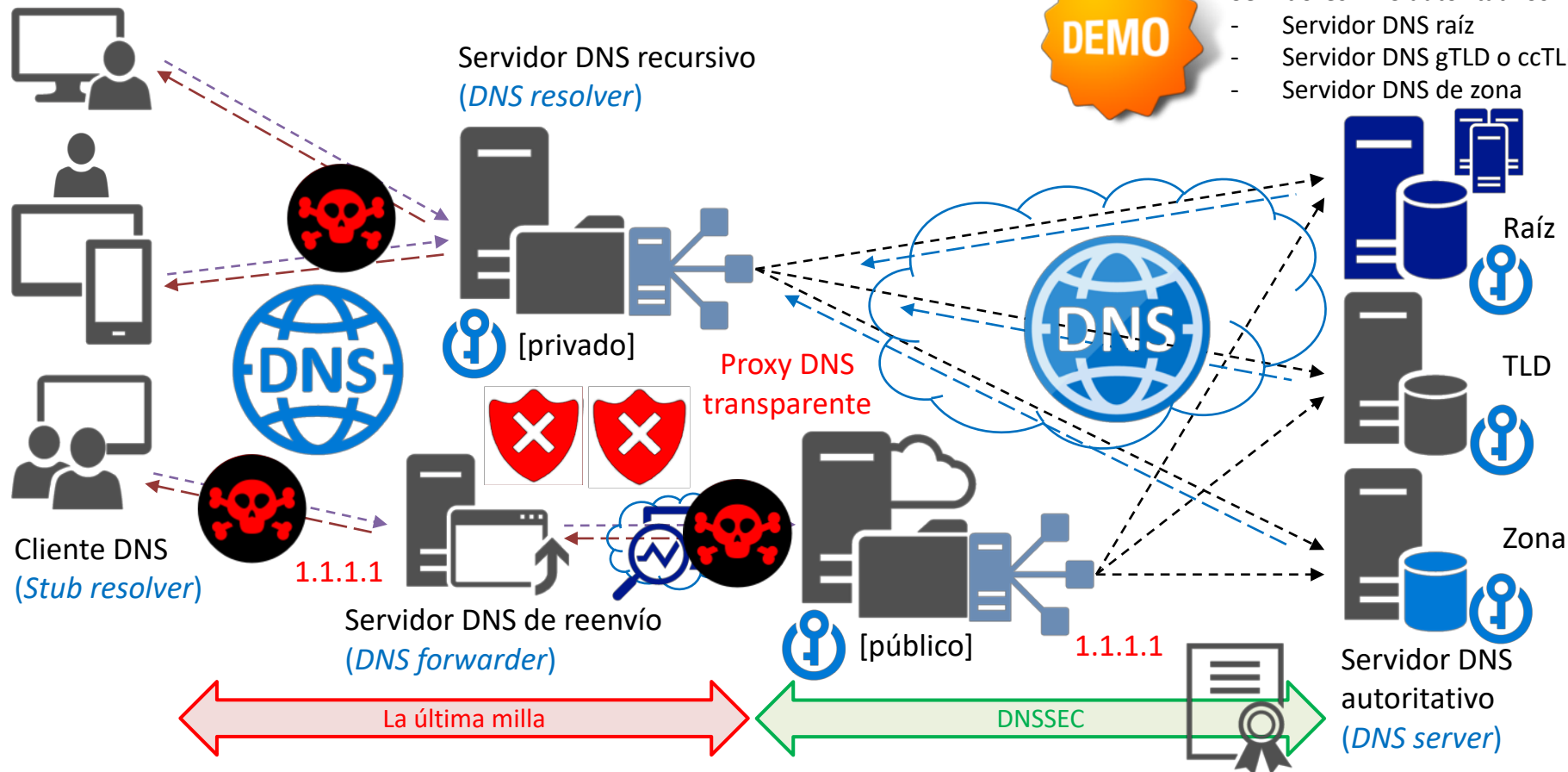
¿Qué tiene que ver esto con DNSSEC?

DNSSEC es compatible con DNS: Dos mundos conviviendo juntos...



Servidores DNS autoritativos:

- Servidor DNS raíz
- Servidor DNS gTLD o ccTLD
- Servidor DNS de zona





Utilizando otros resolvers DNS públicos con soporte para DNSSEC

```
$ dig @8.8.8.8 +dnssec www.isoc.org.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 31624
;; flags: qr rd ra; QUERY: 1, ANSWER: 1,
AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.isoc.org.                IN      A

;; ANSWER SECTION:
www.isoc.org. 13790 IN      A      212.110.167.157

;; Query time: 92 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Jul 06 20:14:33 CEST 2018
;; MSG SIZE rcvd: 57
```

```
$ dig @8.8.8.8 +dnssec www.isoc.org.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 48091
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2,
AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;www.isoc.org.                IN      A

;; ANSWER SECTION:
www.isoc.org. 9985 IN      A      212.110.167.157
www.isoc.org. 9985 IN      RRSIG A 7 3 86400
20180723085001 20180709085001 36614 isoc.org.
BkfloyWnC6SOftIs+miL2gxfyADI9JAf... pytdHBTQEzYs=

;; Query time: 1833 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Jul 10 10:08:40 CEST 2018
;; MSG SIZE rcvd: 225
```

Encuentra las diferencias... 😊



**DoH: DNS over HTTPS...
y DoT: DNS over TLS**



Resolvers DNS públicos



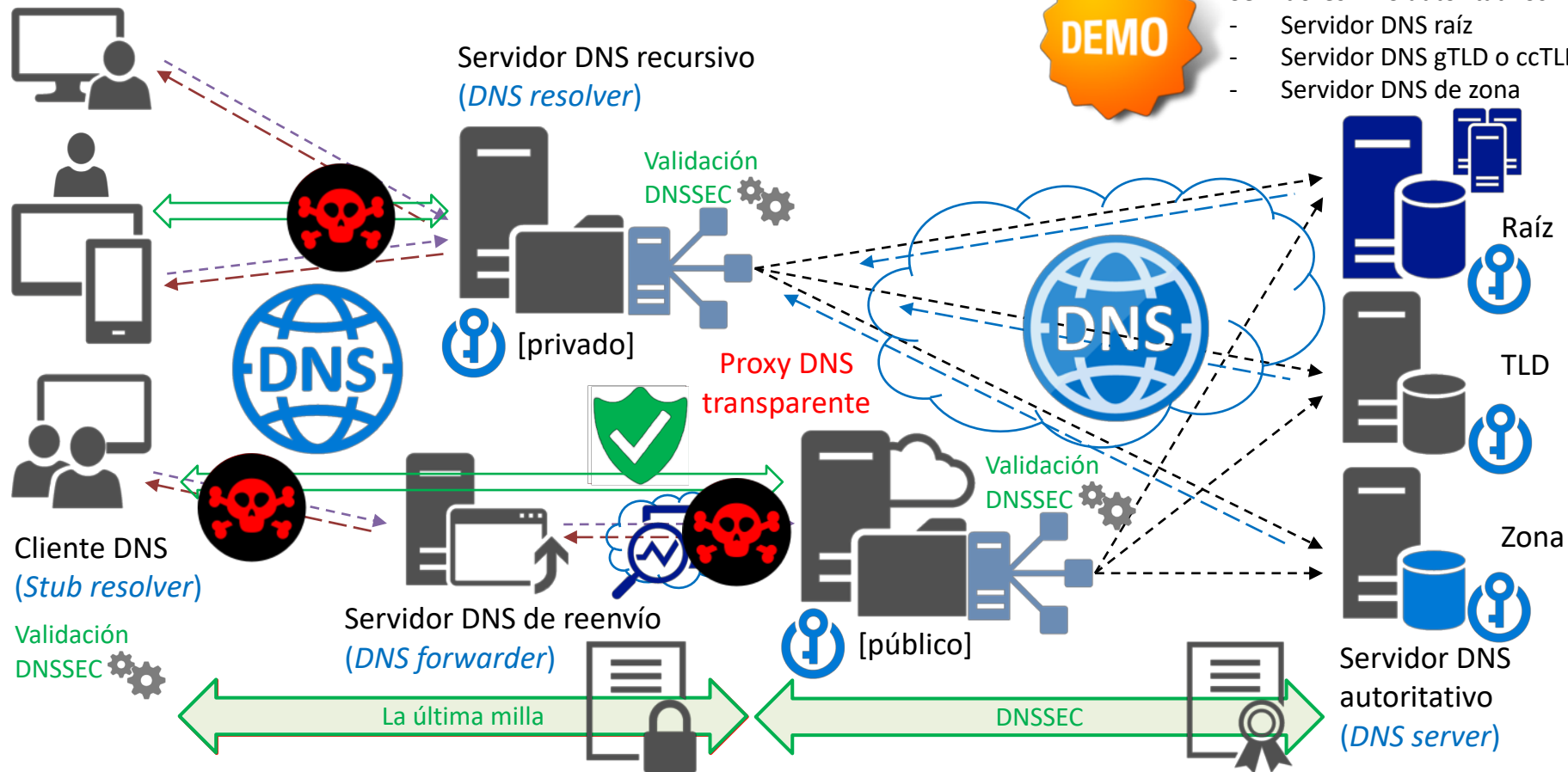
Servicios DNS recursivos públicos

- **Cloudflare: 1.1.1.1 (1.0.0.1)**
 - DNSSEC, DoT, DoH, DNSCrypt
 - DNS over TLS (DoT, TCP/853) – TLS 1.2 & 1.3 (cloudflare-dns.com)
 - DNS over HTTPS (DoH, TCP/443) – TLS 1.2 & 1.3 (<https://cloudflare-dns.com/dns-query>)
 - HTTP/2 over TCP using UDP wireformat / JSON
- **Google: 8.8.8.8 (8.8.4.4)**
 - DNSSEC, DoT, DoH, DNSCrypt
- **Quad9 (IBM et.al.): 9.9.9.9 (9.9.9.10)**
 - DNSSEC, DoT, DoH, DNSCrypt
- **Verisign: 64.6.64.6 (64.6.65.6)**
 - DNSSEC
- **OpenDNS (Cisco): ...**
 - DNSCrypt



Servidores DNS autoritativos:

- Servidor DNS raíz
- Servidor DNS gTLD o ccTLD
- Servidor DNS de zona





Conclusiones

Sólo hemos abierto la Caja de Pandora...



Después de construir todo el ecosistema de DNSSEC...

DNSSEC:

La última
milla...



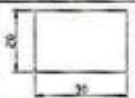
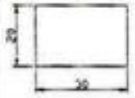
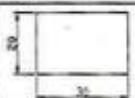
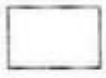


XII Jornadas STIC CCN-CERT

"Ciberseguridad, hacia una respuesta y disuasión efectivas"

Conclusiones

La evolución pedagógica qui permitirá alcanzar el 100% de éxito en las aulas

1990		Calcula el área de este gráfico
1995		Calcula el área de este rectángulo
2000		1. ¿Cuánto mide la base b de este rectángulo? 2. ¿Cuánto mide la altura a de este rectángulo? 3. Calcula el área de este rectángulo multiplicando b por a
2005		Marca con una x el área de este rectángulo 100 ☐ 400 ☐ 600 ☐
2010		Marca con una x el área de este rectángulo 600 ☐
2018		Si no es mucho pedir, colorea el rectángulo con el color que más te guste. Si no, haz lo que te apetezca pero respetando las normas de convivencia.





Eventos relevantes en DNSSEC durante 2018

KSK2010 (19036) --> KSK2017 (20326) - RFC 5011

- **Renovación de la KSK de la zona raíz (Oct 11, 2018)**
 - En Oct 11, 2017, 6-8% de los resolvers sólo confiaban en la KSK antigua (RFC8145)
 - La primera renovación de la KSK raíz desde su generación en 2010
 - <https://www.icann.org/kskroll>
- **"Measuring the KSK Roll" (Sep 2018) & "Analyzing the KSK roll" (Oct 2018)**
 - <https://blog.apnic.net/2018/09/28/measuring-the-ksk-roll/>
 - <https://blog.apnic.net/2018/10/31/analyzing-the-ksk-roll/>
- **ICANN 63 (Barcelona): Oct 20-25, 2018 – DNSSEC Workshop**
 - <https://63.schedule.icann.org/meetings/901549>



ICANN 63
BARCELONA



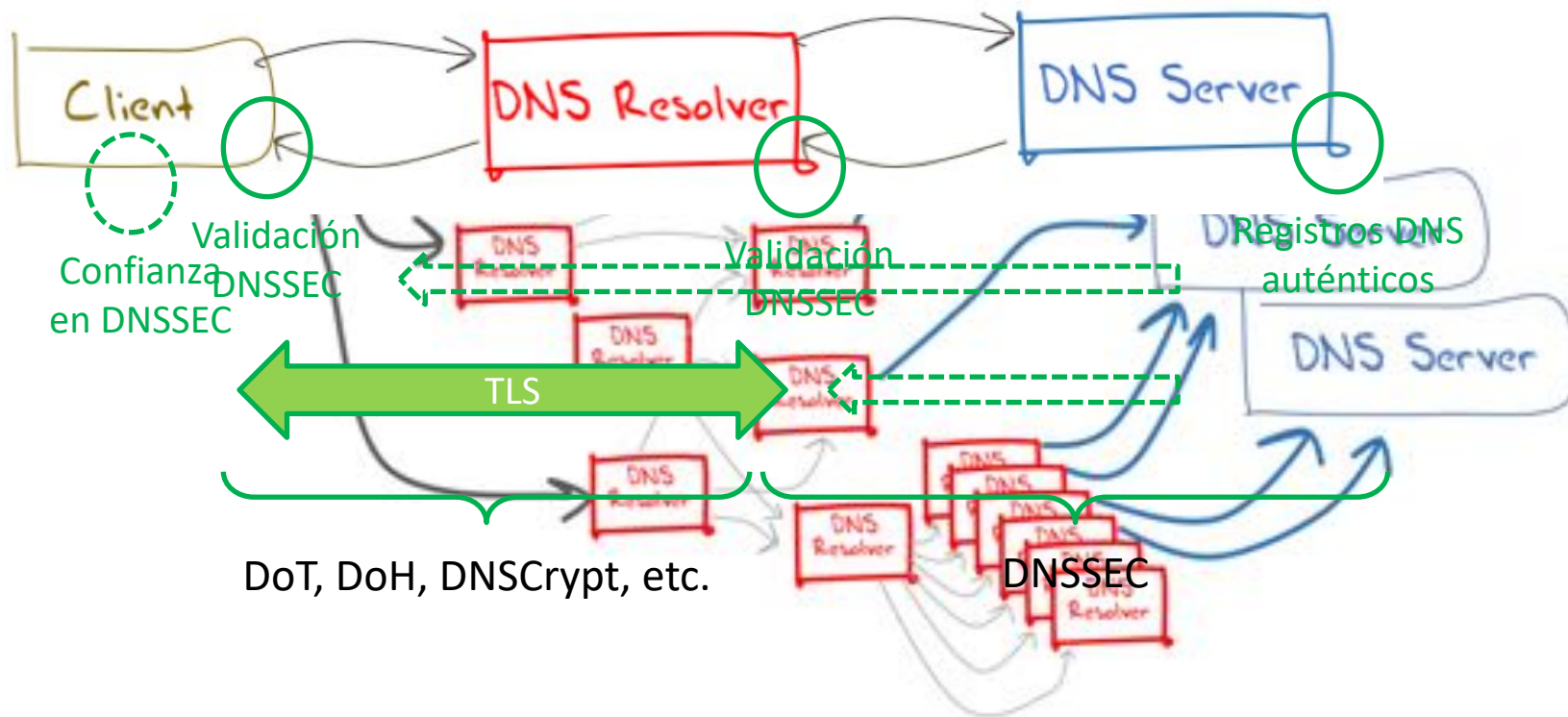
Conclusiones: DNSSEC y DoT/DoH/...

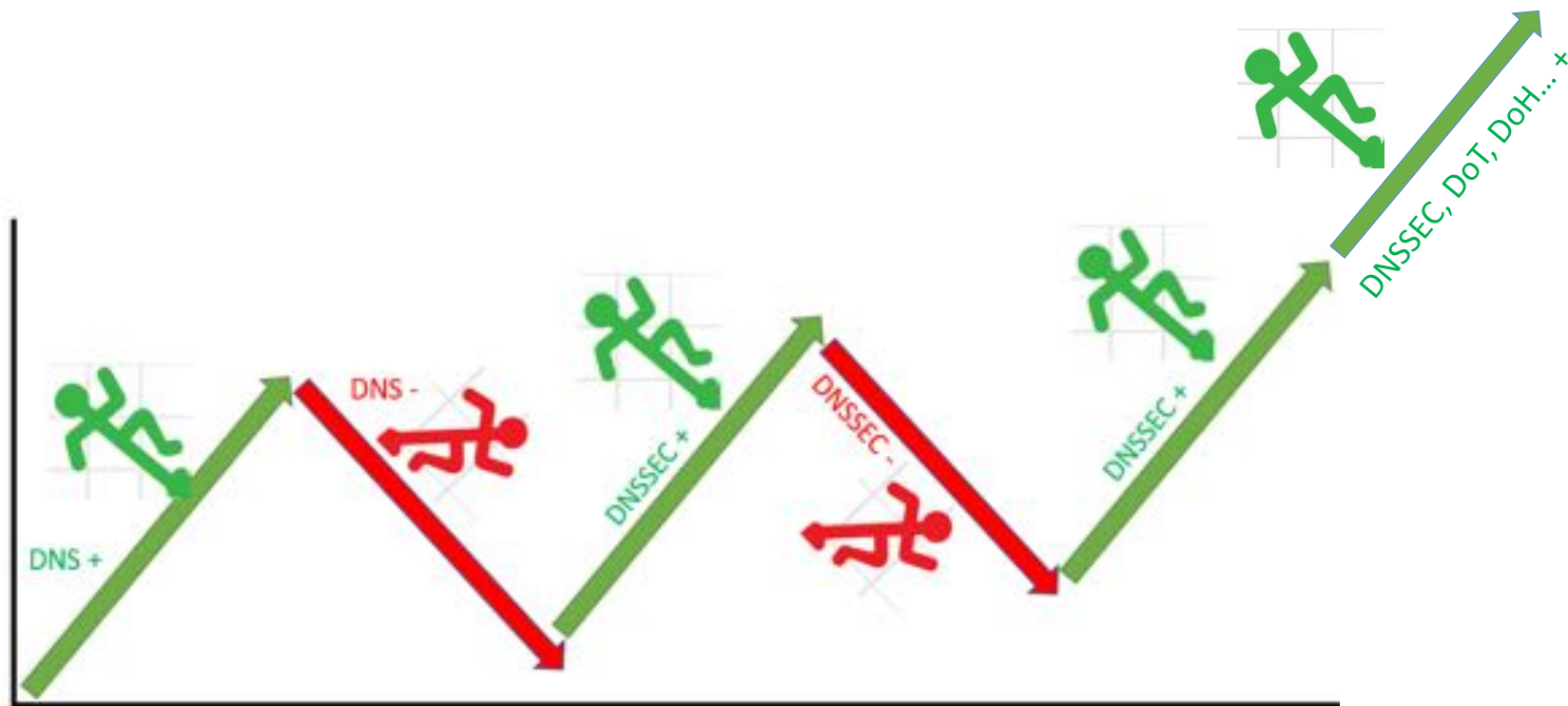
Dos mundos complementarios...

- **DNSSEC**
 - Autenticidad del origen y de los datos (actuales)
 - Integridad entre el resolver y el servidor DNS autoritativo
- **DNS over TLS (DoT) o DNS over HTTPS (DoH)**
 - Autenticación y cifrado del servicio (o servidor)
 - Privacidad e integridad entre el cliente DNS y el resolver
 - <https://dnsprivacy.org>
 - "La última (o la primera) milla"
- **DANE: DNS-Based Authentication of Named Entities**
 - Integración entre certificados digitales de TLS y zonas DNS



Confianza en la validación de las respuestas de DNSSEC

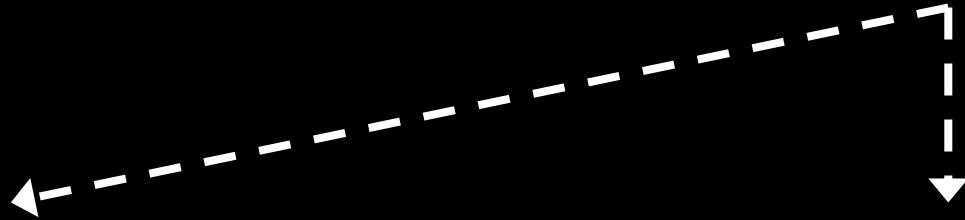




**¿Quién se plantea hacer uso de
DNSSEC?**

Firmado de zona

Validación



Utilizo DNSSEC (Validación)

Valido zonas con DNSSEC (DNS resolver)

NO

SI

Proporciono DNSSEC (Firma de zona)
Publico zonas con DNSSEC (DNS autoritativo)

NO

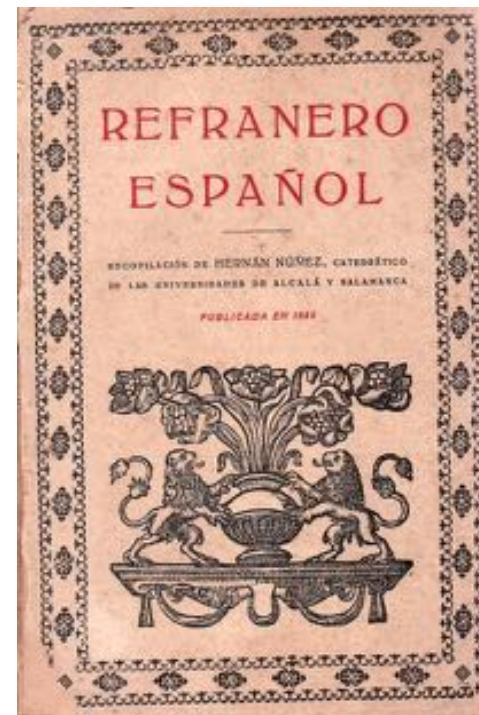


SI



“XXX”

El refranero español





Referencias



Guías DNSSEC / DNS

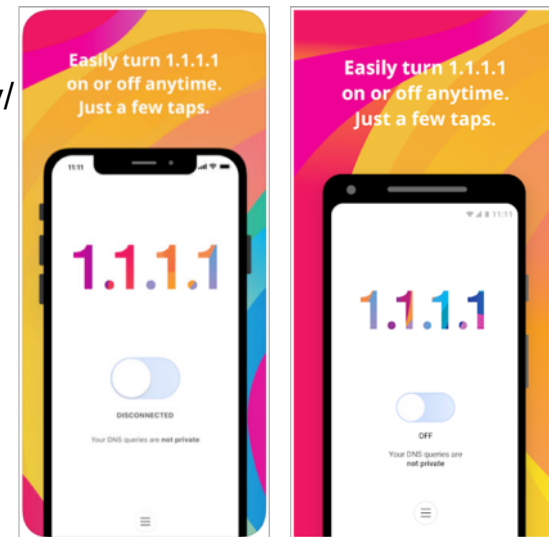
- Estudio del estado de DNSSEC en España – Oct 2018
 - <https://www.incibe-cert.es/guias-y-estudios/estudios/estudio-del-estado-dnssec-espana>
- Guía de implantación y buenas prácticas de DNSSEC – Oct 2018
 - <https://www.incibe-cert.es/guias-y-estudios/guias/guia-implantacion-y-buenas-practicas-dnssec>
- CCN-STIC-664 Passive DNS – Ago 2014
 - <https://www.ccn-cert.cni.es/series-ccn-stic/600-guias-de-otros-entornos/461-ccn-stic-664-passive-dns-dl/file.html>
- CCN-STIC-663 Seguridad en DNS (BIND) – Abr 2014
 - <https://www.ccn-cert.cni.es/series-ccn-stic/600-guias-de-otros-entornos/459-ccn-stic-663-seguridad-en-dns-bind/file.html>
- Guía de Seguridad en servicios DNS – Abr 2014
 - <https://www.incibe-cert.es/guias-y-estudios/guias/guia-seguridad-dns>



Referencias

1.1.1.1 (Cloudflare)

- "Announcing 1.1.1.1: the fastest, privacy-first consumer DNS service" (April 1, 2018)
 - <https://blog.cloudflare.com/announcing-1111/>
 - <https://blog.cloudflare.com/dns-resolver-1-1-1-1>
- "Fixing reachability to 1.1.1.1, GLOBALLY!" (Apr 2018)
 - <https://blog.cloudflare.com/fixing-reachability-to-1-1-1-1-globally/>
- DNS over TLS (DoT)
 - <https://tools.ietf.org/html/rfc7858>
 - <https://developers.cloudflare.com/1.1.1.1/dns-over-tls/>
- DNS (Queries) over HTTPS (DoH)
 - <https://tools.ietf.org/html/rfc8484>
 - <https://developers.cloudflare.com/1.1.1.1/dns-over-https/>
- "DNSEC: An Introduction" (Oct 2014)
 - <https://blog.cloudflare.com/dnssec-an-introduction/>





Referencias

APNIC

APNIC Lab

- "Why DNSSEC deployment remains so low" (Dec 2017)
 - <https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/>
- "Bringing DNS security and privacy to the end user" (Feb 2018)
 - <https://blog.apnic.net/2018/02/07/bringing-dns-security-privacy-end-user/>
- "Sunrise DNS over TLS, sunset DNSSEC?" & "DNSSEC and DNS over TLS" (Aug 2018)
 - <https://blog.apnic.net/2018/08/17/sunrise-dns-over-tls-sunset-dnssec/>
 - <https://blog.apnic.net/2018/08/20/dnssec-and-dns-over-tls/>
- "DOH! DNS over HTTPS explained" (Oct 2018)
 - <https://blog.apnic.net/2018/10/12/doh-dns-over-https-explained/>



Referencias

More RFCs...

- "DNS Query Name Minimisation to Improve Privacy" (Mar 2016)
 - <https://tools.ietf.org/html/rfc7816>
- "CHAIN Query Requests in DNS" (Jun 2016)
 - <https://tools.ietf.org/html/rfc7901>
- "DNSSEC Roadblock Avoidance" (Nov 2016)
 - <https://tools.ietf.org/html/rfc8027>
- "DNS over Datagram Transport Layer Security (DTLS)" (Feb 2017)
 - <https://tools.ietf.org/html/rfc8094>
- "Aggressive Use of DNSSEC-Validated Cache" (Jul 2017)
 - <https://tools.ietf.org/html/rfc8198>
- "Usage Profiles for DNS over TLS and DNS over DTLS" (Mar 2018)
 - <https://tools.ietf.org/html/rfc8310>
- DANE: DNS-Based Authentication of Named Entities
 - <https://tools.ietf.org/html/rfc7671>





Referencias

Herramientas (<https://dnsflagday.net...> :-)

- **DNSSEC analyzer (Verisign)**
 - <https://dnssec-analyzer.verisignlabs.com>
- **DNS Viz (Sandia & Verisign)**
 - <http://dnsviz.net>
 - <https://github.com/dnsviz/dnsviz>
- **1.1.1.1 Connection Information**
 - <https://cloudflare-dns.com/help/>
- **Public DNS resolvers performance**
 - <https://www.dnsperf.com/#!/dns-resolvers>
- **DNS Leak**
 - <https://www.dnsleaktest.com>





www.dinosec.com
@dinosec

Mónica Salas
monica@dinosec.com

Raúl Siles
raul@dinosec.com





ccn-cert
centro criptológico nacional



¿Preguntas?

DinoSec

www.dinosec.com
[@dinosec](https://twitter.com/dinosec)



¡Muchas gracias!

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- oc.ccn.cni.es

➤ Síguenos en



ccn-cert
centro criptológico nacional

