ION BUCHAREST 2016

https://www.flickr.com/photos/ntrinkhaus/10594770836 CC BY NC

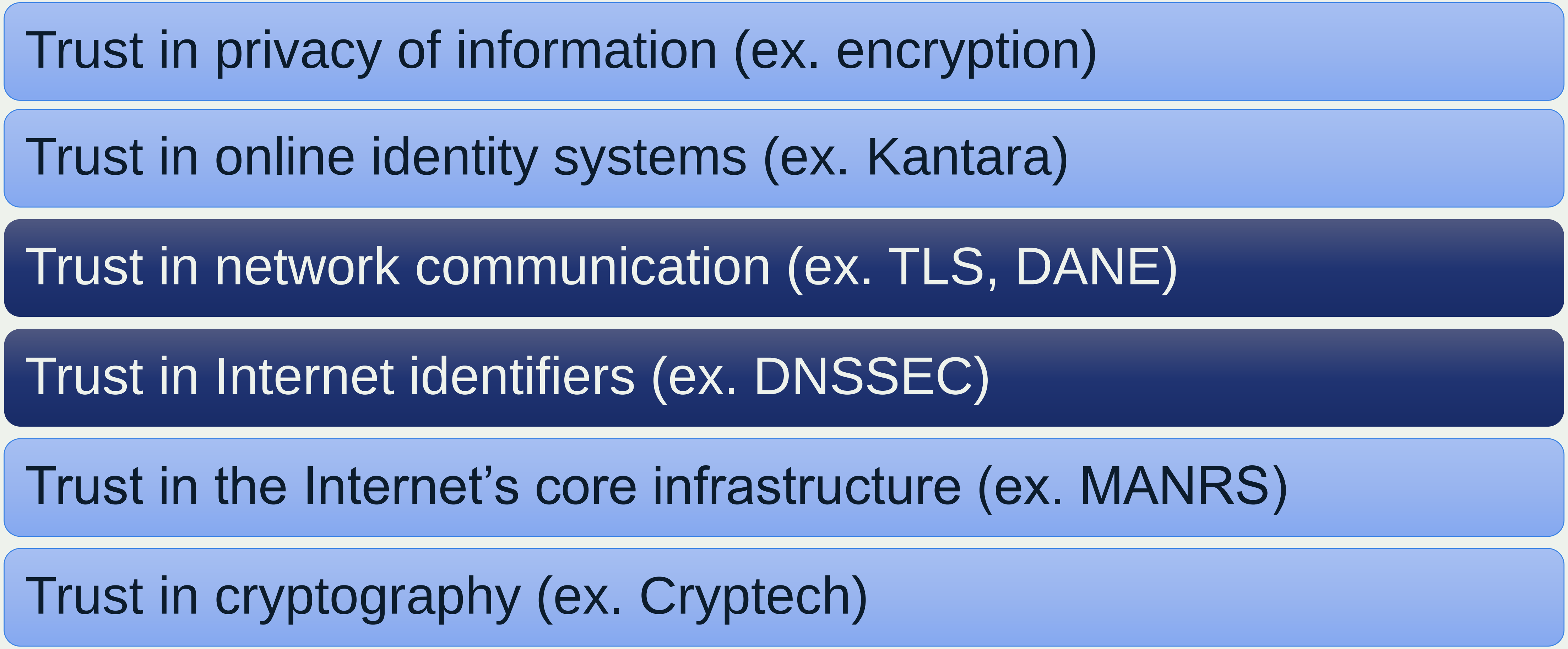
Deploying DNSSEC

ION Bucharest

October 12, 2016

Dan York, CISSP
DNSSEC Program Manager – york@isoc.org

Trusted Internet



- Trust in privacy of information (ex. encryption)
- Trust in online identity systems (ex. Kantara)
- Trust in network communication (ex. TLS, DANE)
- Trust in Internet identifiers (ex. DNSSEC)
- Trust in the Internet’s core infrastructure (ex. MANRS)
- Trust in cryptography (ex. Cryptech)

https://www.flickr.com/photos/powerbooktrance/466709245/ CC BY

Email Hijacking

CERT-CC researchers have identified that someone was hijacking email by using DNS cache poisoning of MX records

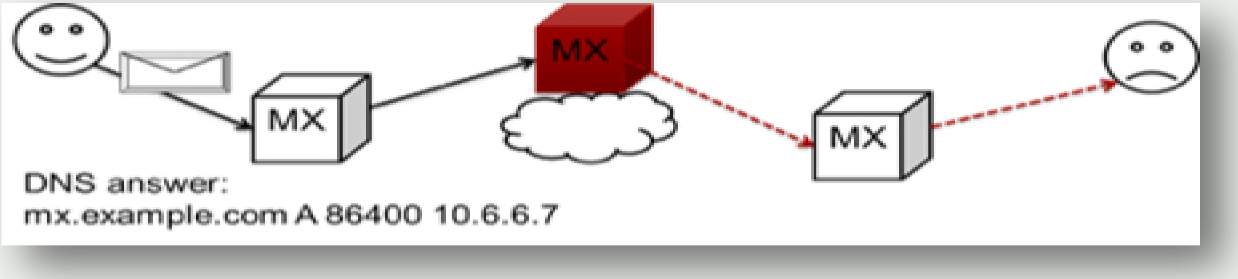
Could be prevented by DNSSEC deployment

CERT-CC (Sept 10, 2014):

- https://www.cert.org/blogs/certcc/post.cfm?EntryID=206

Deploy360 blog post (Sept 12, 2014):

- http://wp.me/p4eijv-5jl



What Problem Is DNSSEC Trying To Solve?

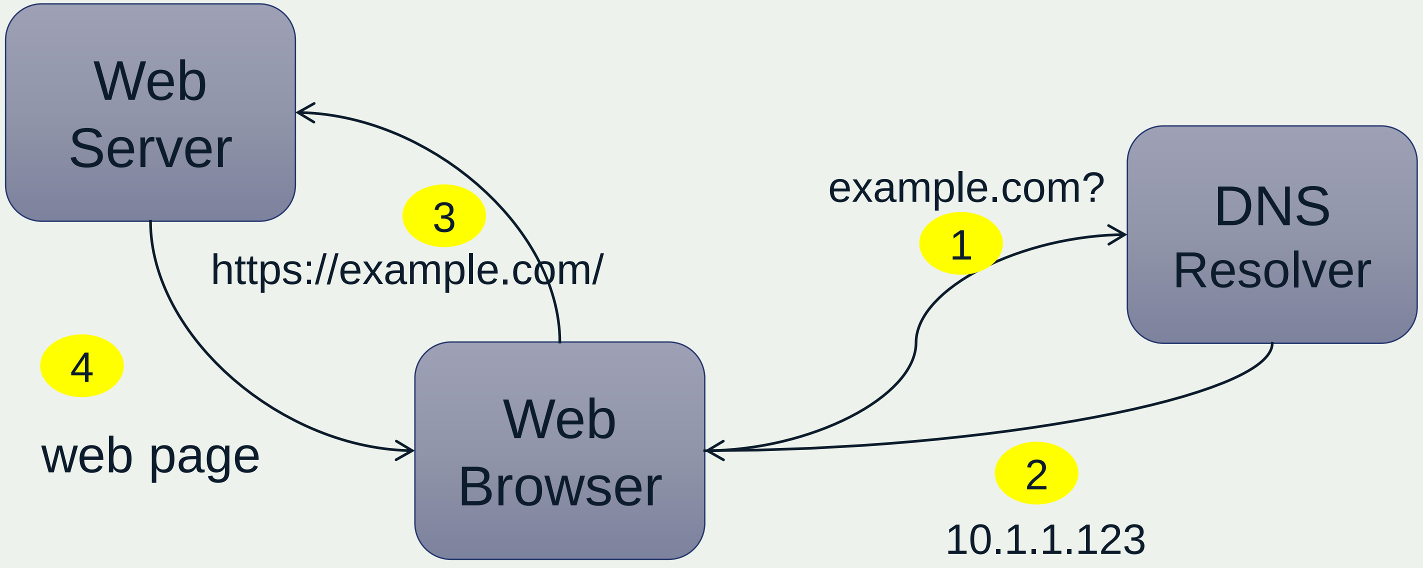
DNSSEC = "DNS Security Extensions"

- Defined in RFCs 4033, 4034, 4035
- Operational Practices: RFC 4641

Ensures that the information entered into DNS by the domain name holder is the SAME information retrieved from DNS by an end user.

Let's walk through an example to explain…

A Normal DNS Interaction

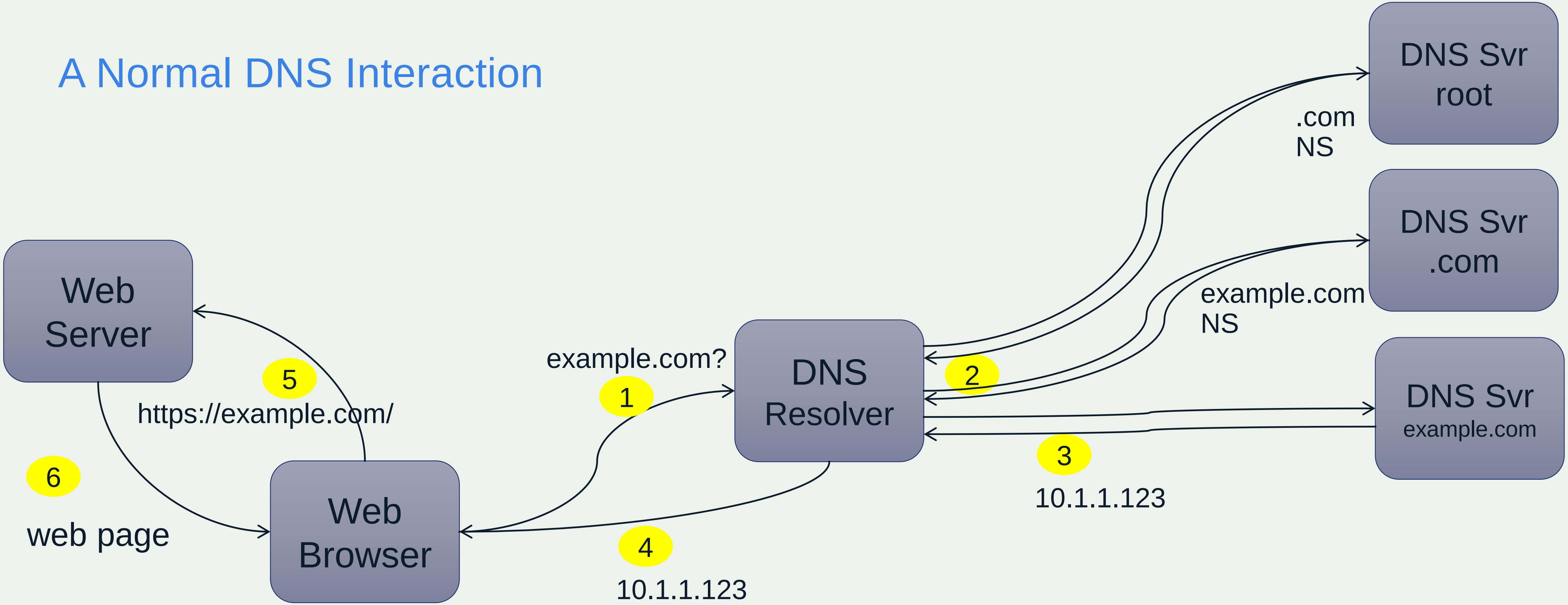


Resolver checks its local *cache.* If it has the answer, it sends it back.

example.com 10.1.1.123

If not…

A Normal DNS Interaction

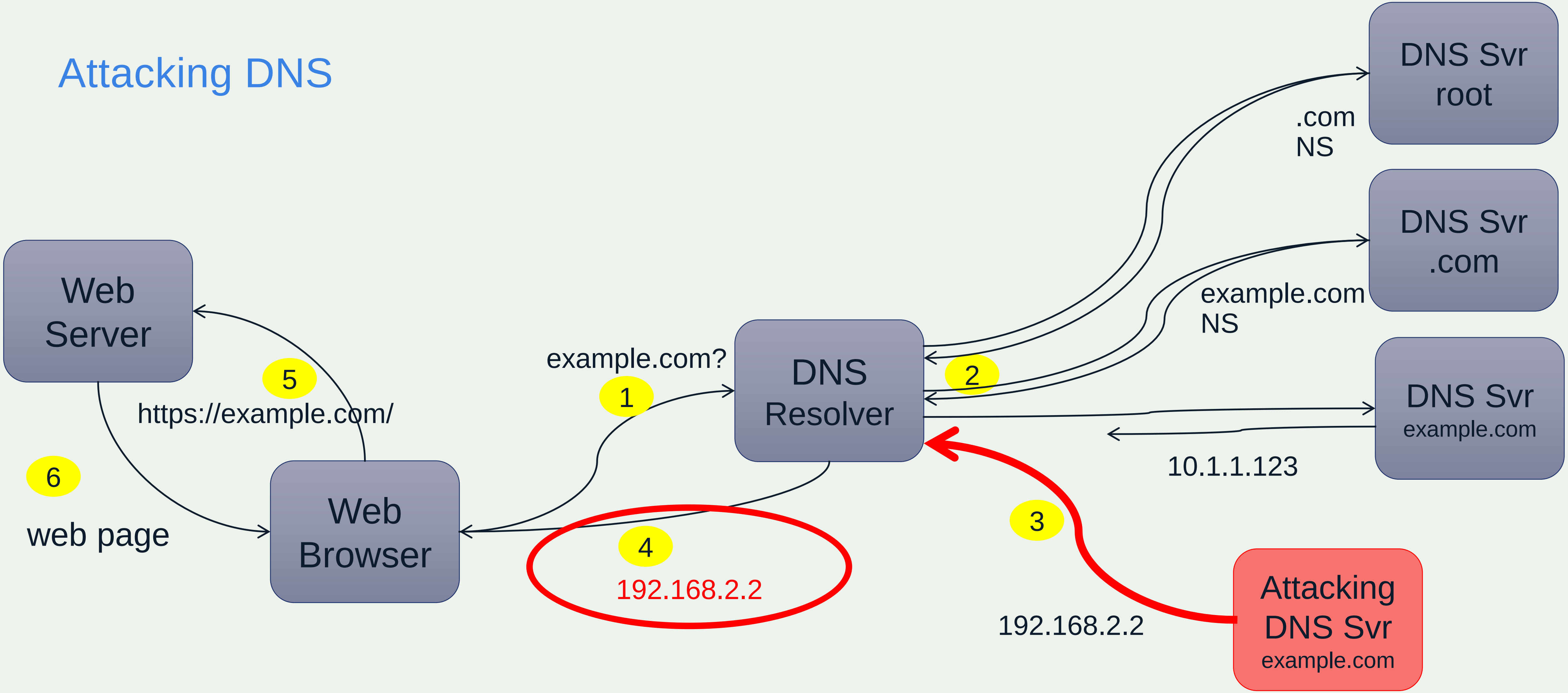


DNS Works On Speed

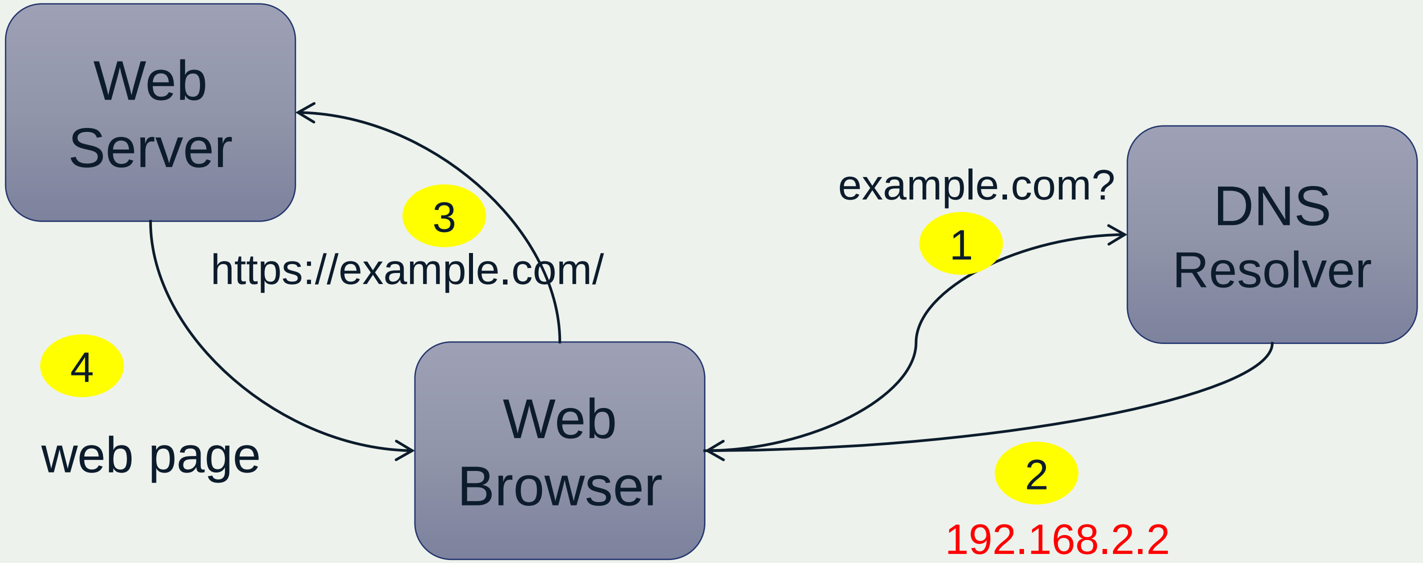
First result received by a DNS resolver is treated as the correct answer.

Opportunity is there for an attacker to be the first one to get an answer to the DNS resolver, either by:
Getting to the correct point in the network to provide faster responses;
Blocking the responses from the legitimate servers (ex. executing a Denial of Service attack against the legitimate servers to slow their responses)

Attacking DNS



A Poisoned Cache



Resolver ***cache*** now has wrong data:

example.com 192.168.2.2

This stays in the cache until the Time-To-Live (TTL) expires!

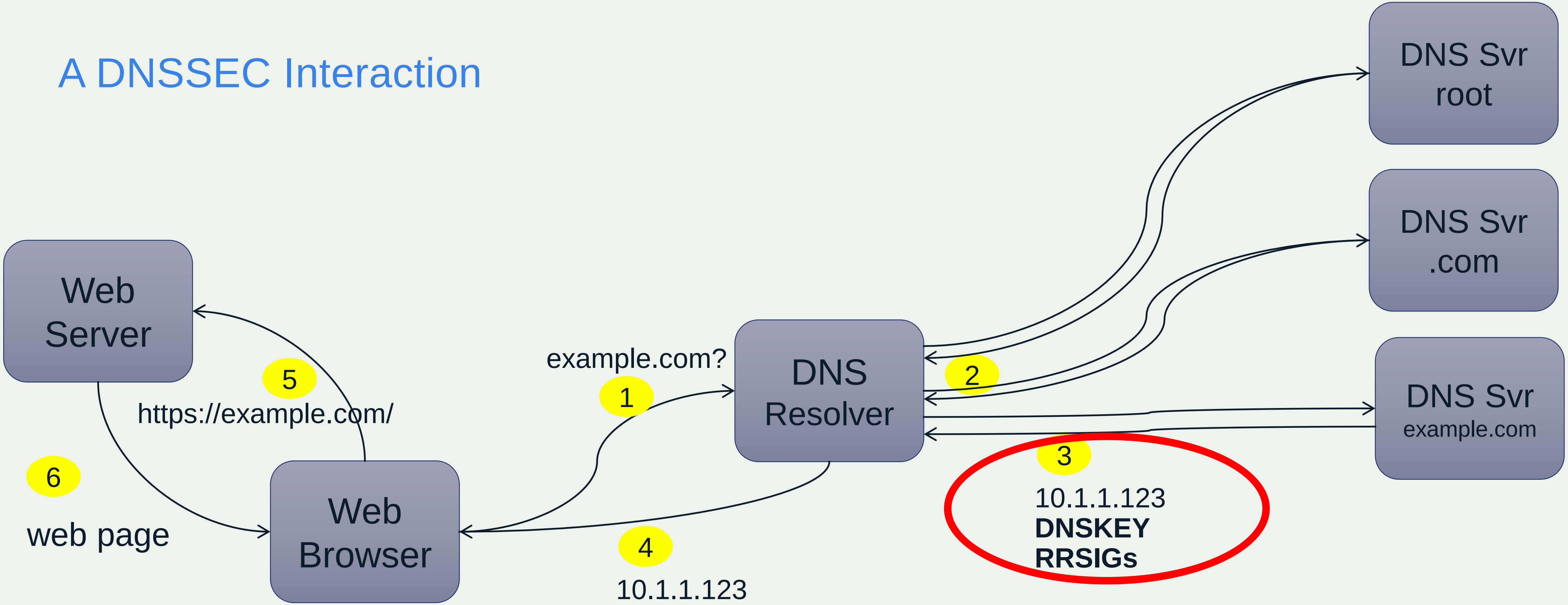
How Does DNSSEC Help?

DNSSEC introduces new DNS records for a domain:

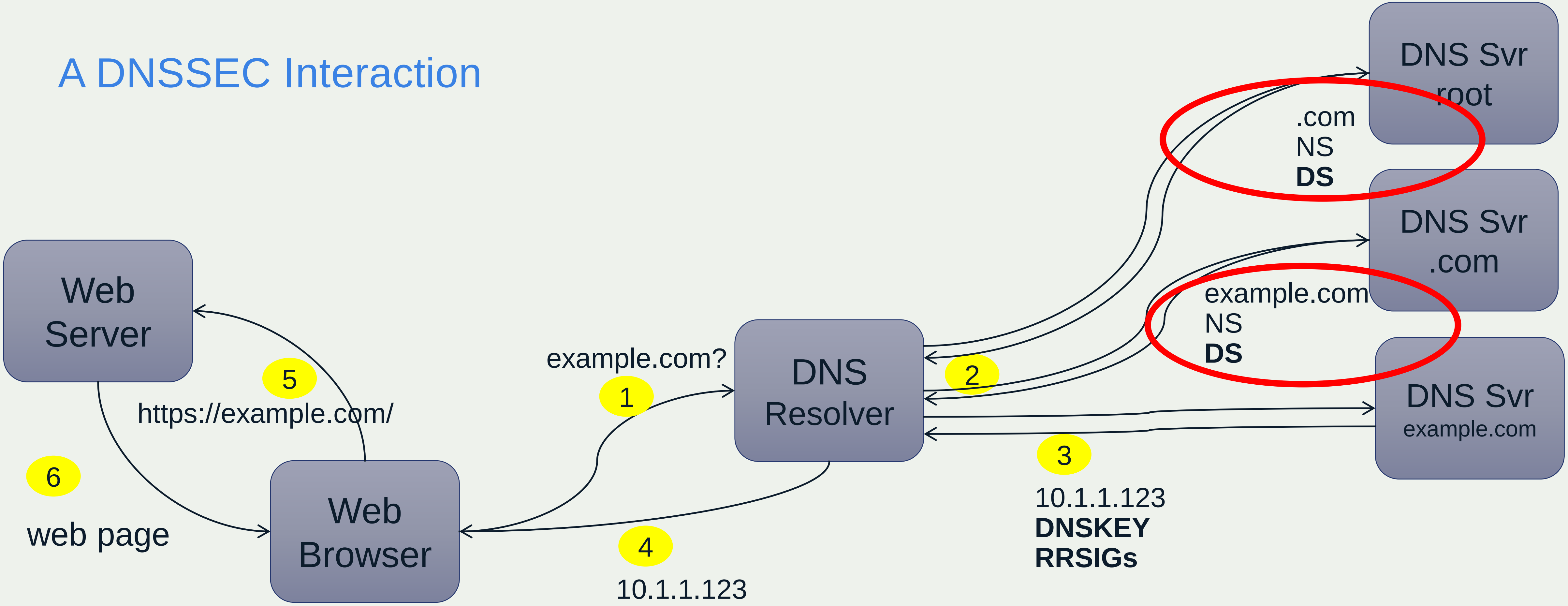
- **RRSIG** – a signature ("hash") of a set of DNS records
- **DNSKEY** – a public key that a resolver can use to validate RRSIG

A DNSSEC-validating DNS resolver:
Uses DNSKEY to perform a hash calculation on received DNS records
Compares result with RRSIG records. If results match, records are the same as those transmitted. If the results do NOT match, they were potentially changed during the travel from the DNS server.

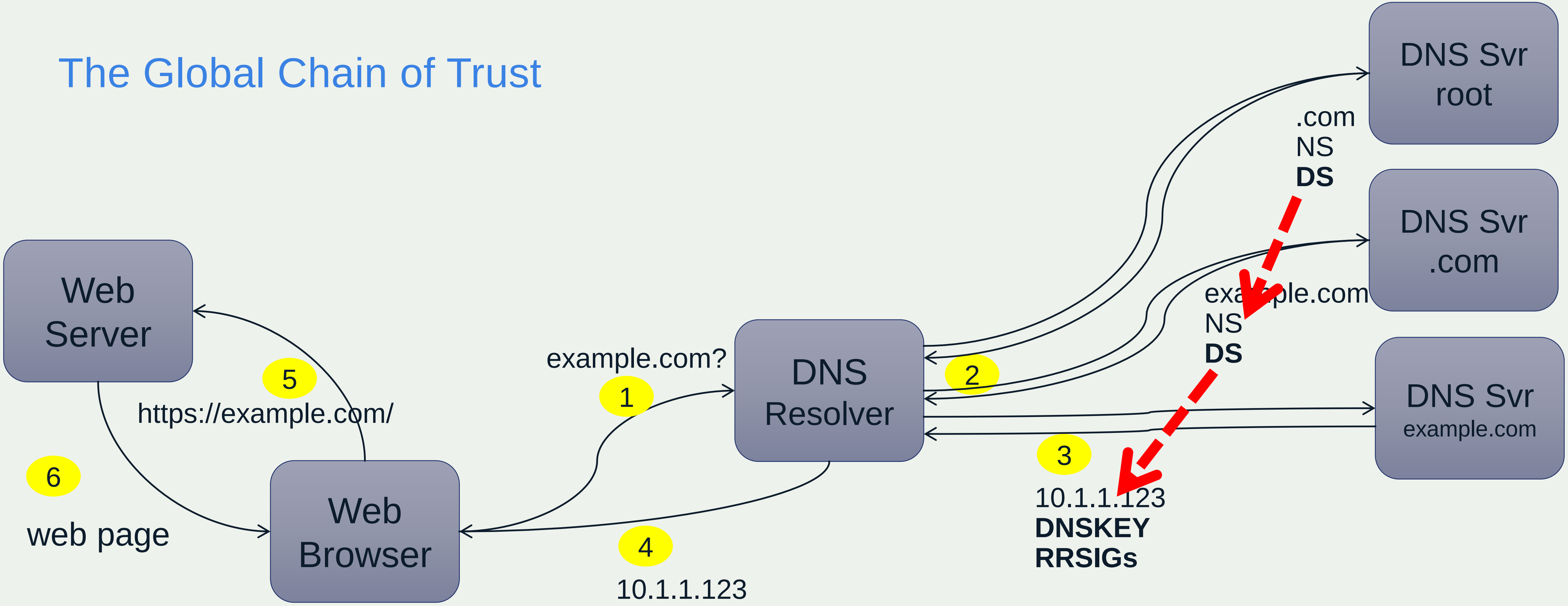
A DNSSEC Interaction



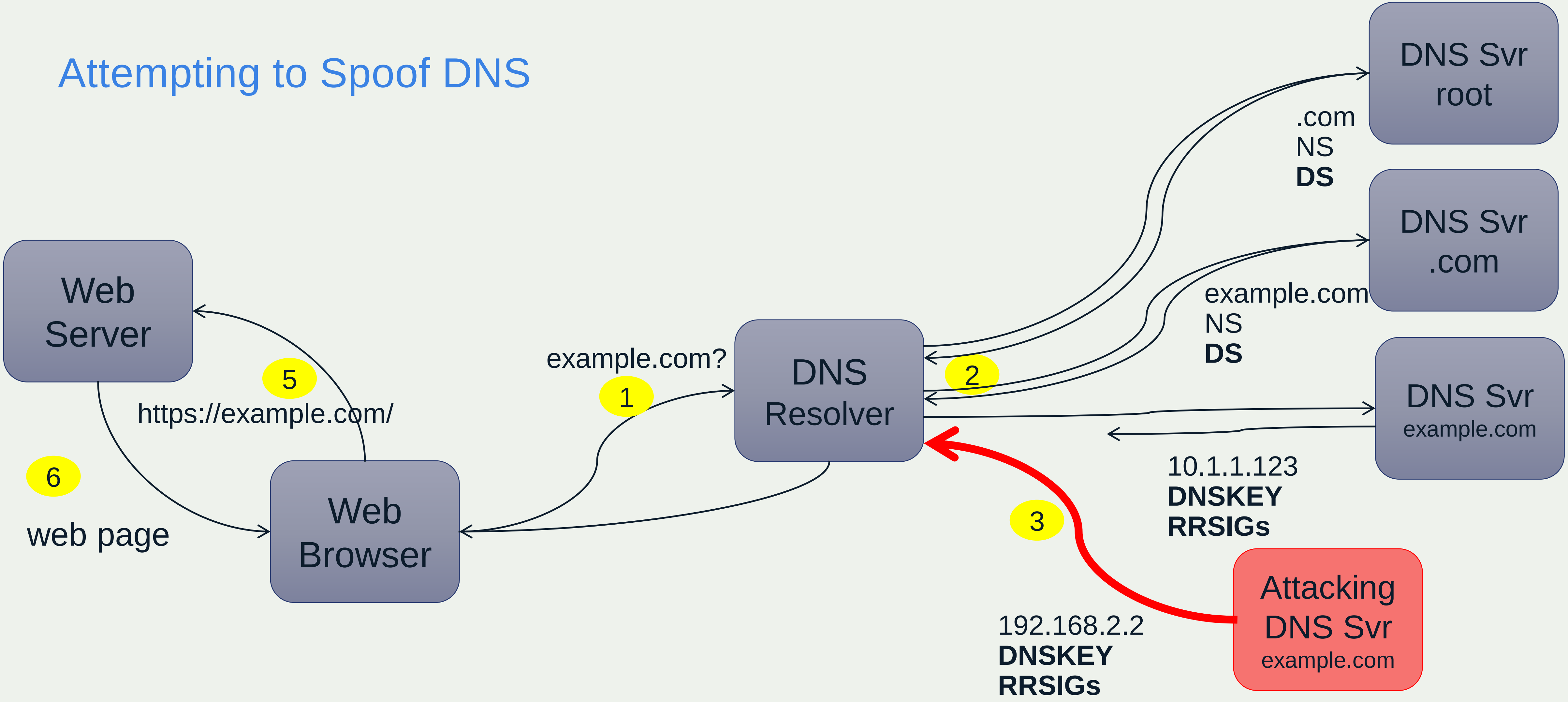
A DNSSEC Interaction



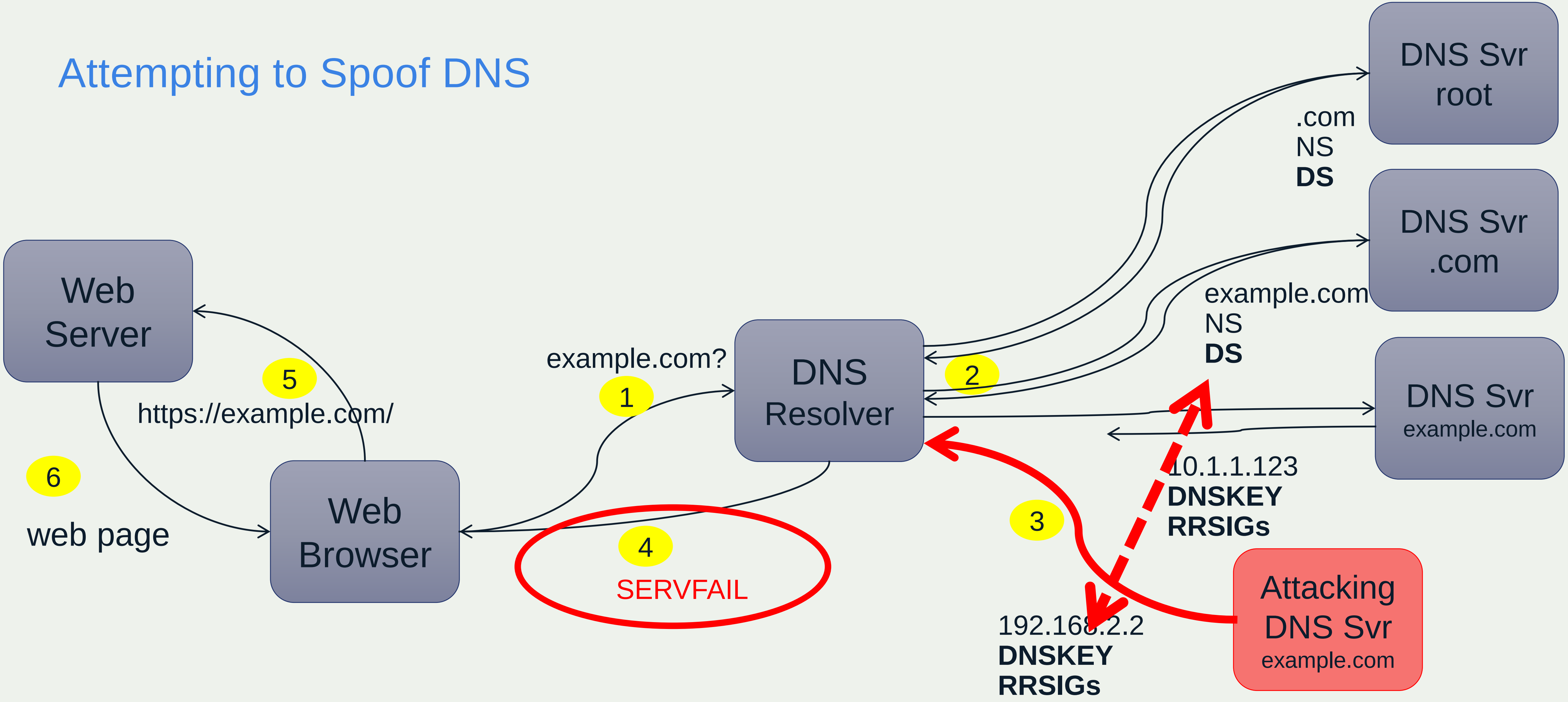
The Global Chain of Trust



Attempting to Spoof DNS



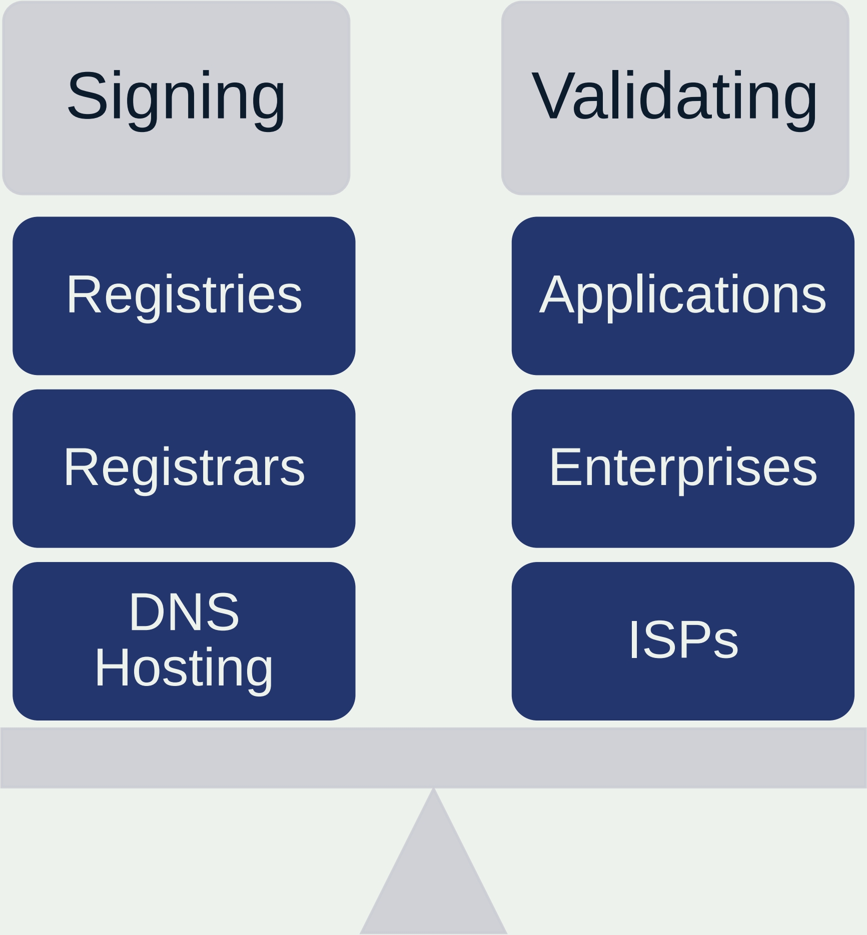
Attempting to Spoof DNS



What DNSSEC Proves:

- "These ARE the IP addresses you are looking for."
  (or they are not)
- Ensures that information entered into DNS by the domain name holder (or the operator of the DNS hosting service for the domain) is the SAME information that is received by the end user.

The Two Parts of DNSSEC



Signing

Registries

Registrars

DNS Hosting

Validating

Applications

Enterprises

ISPs

What DNSSEC Proves:

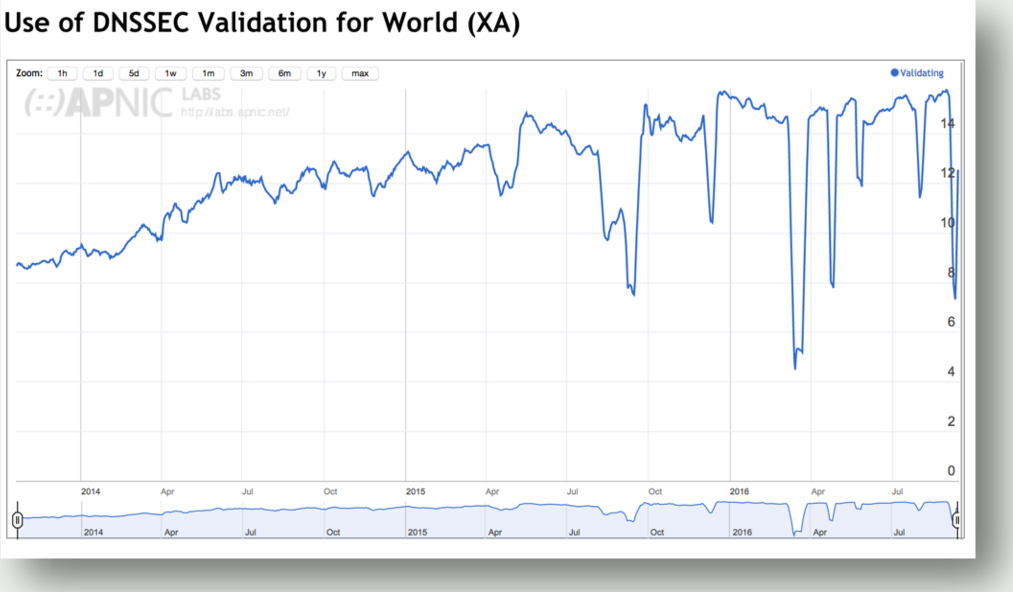
- "These ARE the IP addresses you are looking for."
  (or they are not)
- Ensures that information entered into DNS by the domain name holder (or the operator of the DNS hosting service for the domain) is the SAME information that is received by the end user.

DNSSEC Validation – Current State

- About 15% of all global DNS queries validated

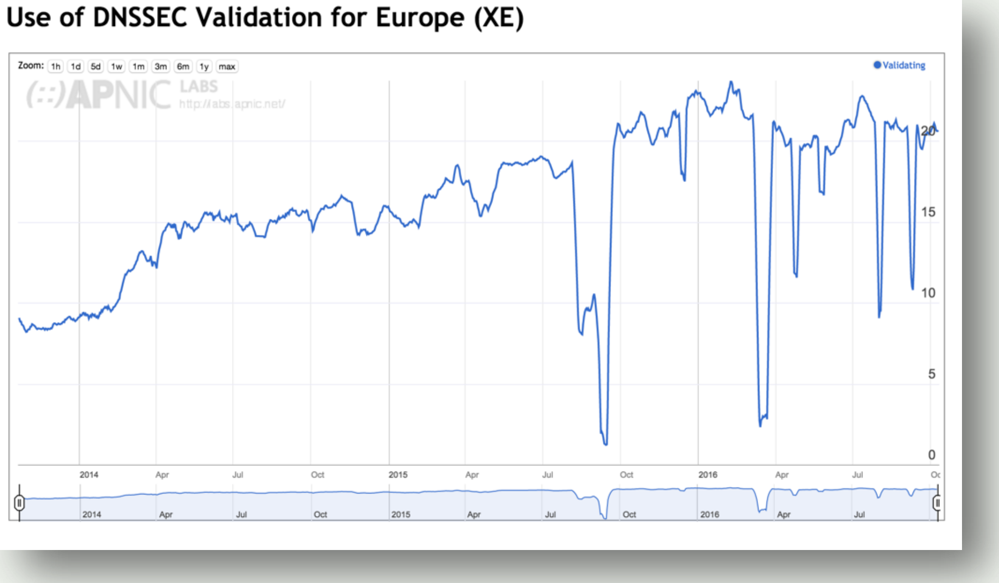
- ~20% of all European DNS queries validated

- All major DNS resolvers support DNSSEC validation – often with a simple config change



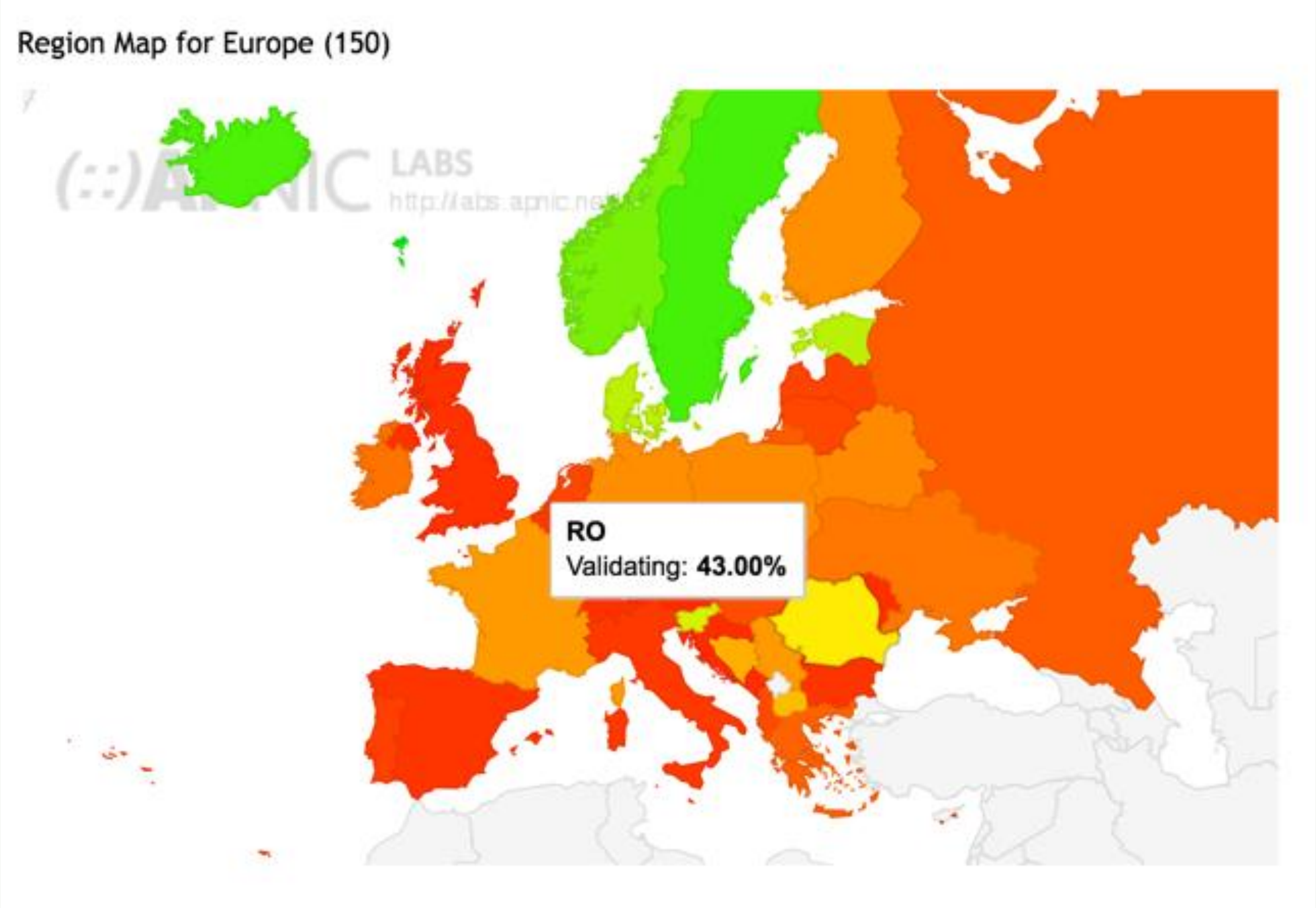
Use of DNSSEC Validation for World (XA)

http://stats.labs.apnic.net/dnssec



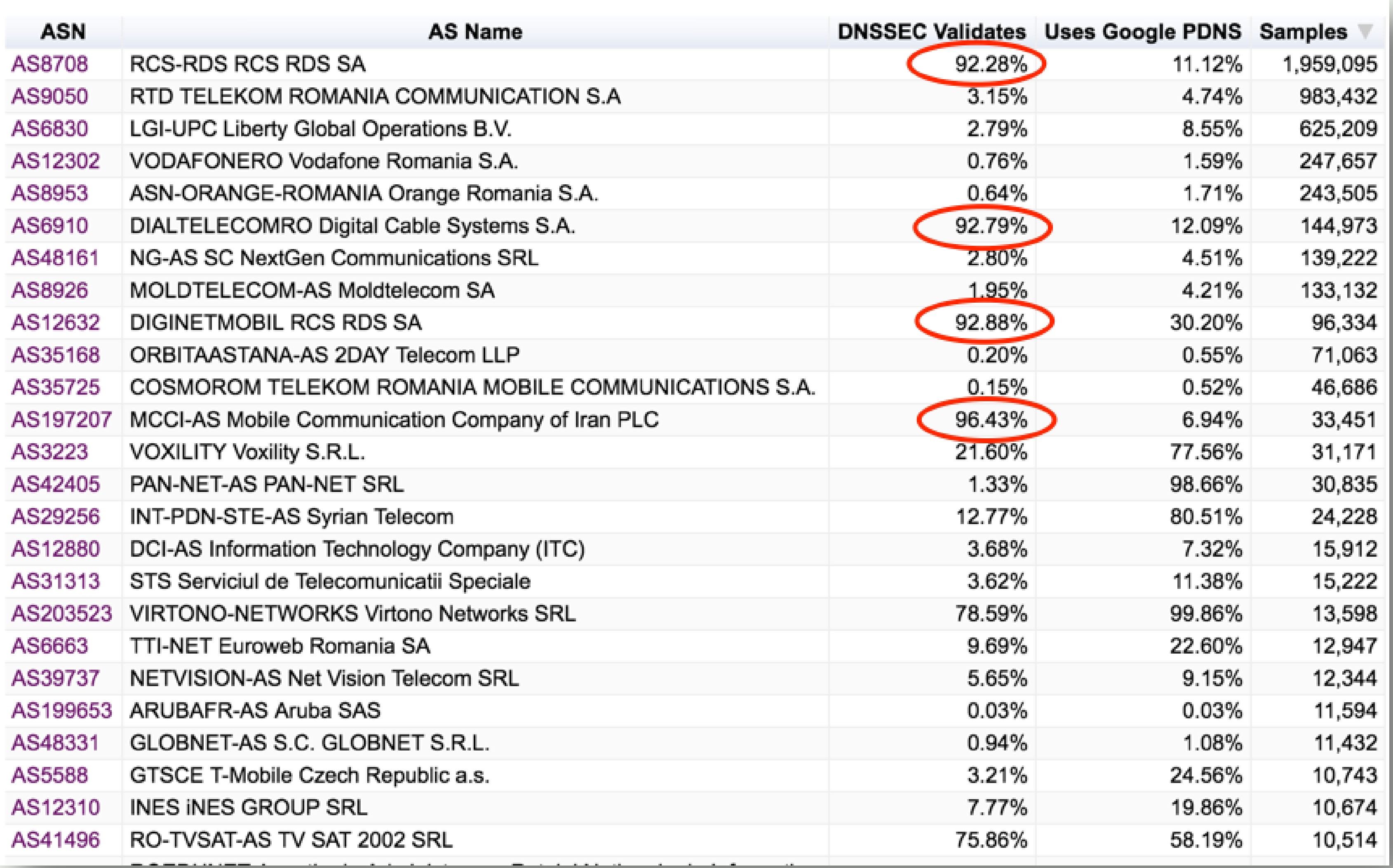
Use of DNSSEC Validation for Europe (XE)

DNSSEC Validation – Romania


Region Map for Europe (150)

http://stats.labs.apnic.net/dnssec

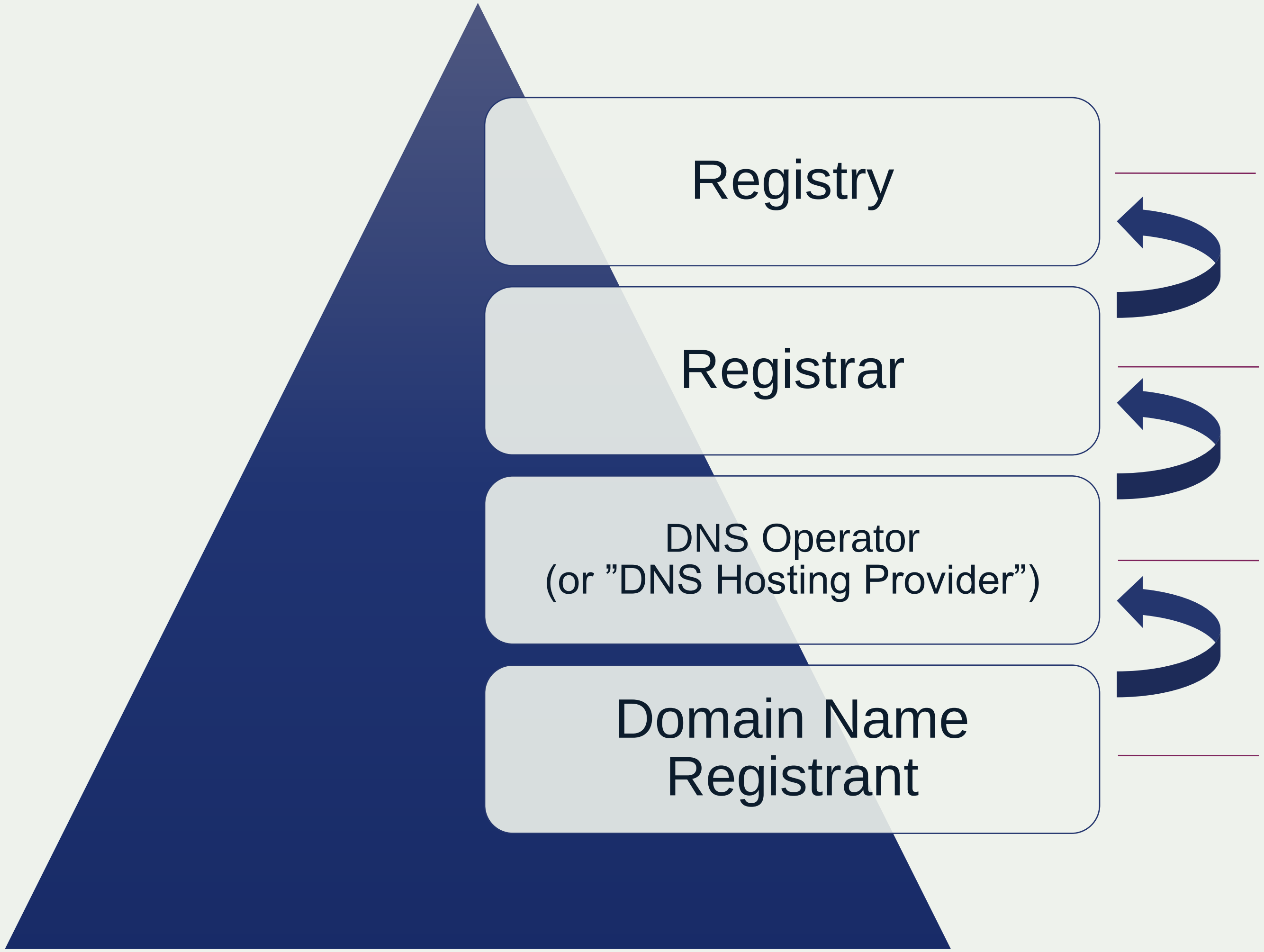
DNSSEC Validation – Romania



ASN	AS Name	DNSSEC Validates	Uses Google PDNS	Samples
AS8708	RCS-RDS RCS RDS SA	92.28%	11.12%	1,959,095
AS9050	RTD TELEKOM ROMANIA COMMUNICATION S.A	3.15%	4.74%	983,432
AS6830	LGI-UPC Liberty Global Operations B.V.	2.79%	8.55%	625,209
AS12302	VODAFONERO Vodafone Romania S.A.	0.76%	1.59%	247,657
AS8953	ASN-ORANGE-ROMANIA Orange Romania S.A.	0.64%	1.71%	243,505
AS6910	DIALTELECOMRO Digital Cable Systems S.A.	92.79%	12.09%	144,973
AS48161	NG-AS SC NextGen Communications SRL	2.80%	4.51%	139,222
AS8926	MOLDTELECOM-AS Moldtelecom SA	1.95%	4.21%	133,132
AS12632	DIGINETMOBIL RCS RDS SA	92.88%	30.20%	96,334
AS35168	ORBITAASTANA-AS 2DAY Telecom LLP	0.20%	0.55%	71,063
AS35725	COSMOROM TELEKOM ROMANIA MOBILE COMMUNICATIONS S.A.	0.15%	0.52%	46,686
AS197207	MCCI-AS Mobile Communication Company of Iran PLC	96.43%	6.94%	33,451
AS3223	VOXILITY Voxility S.R.L.	21.60%	77.56%	31,171
AS42405	PAN-NET-AS PAN-NET SRL	1.33%	98.66%	30,835
AS29256	INT-PDN-STE-AS Syrian Telecom	12.77%	80.51%	24,228
AS12880	DCI-AS Information Technology Company (ITC)	3.68%	7.32%	15,912
AS31313	STS Serviciul de Telecomunicatii Speciale	3.62%	11.38%	15,222
AS203523	VIRTONO-NETWORKS Virtono Networks SRL	78.59%	99.86%	13,598
AS6663	TTI-NET Euroweb Romania SA	9.69%	22.60%	12,947
AS39737	NETVISION-AS Net Vision Telecom SRL	5.65%	9.15%	12,344
AS199653	ARUBAFR-AS Aruba SAS	0.03%	0.03%	11,594
AS48331	GLOBNET-AS S.C. GLOBNET S.R.L.	0.94%	1.08%	11,432
AS5588	GTSCE T-Mobile Czech Republic a.s.	3.21%	24.56%	10,743
AS12310	INES iNES GROUP SRL	7.77%	19.86%	10,674
AS41496	RO-TVSAT-AS TV SAT 2002 SRL	75.86%	58.19%	10,514

http://stats.labs.apnic.net/dnssec

DNSSEC Signing - The Individual Steps



- Signs TLD
- Accepts DS records
- Publishes/signs records

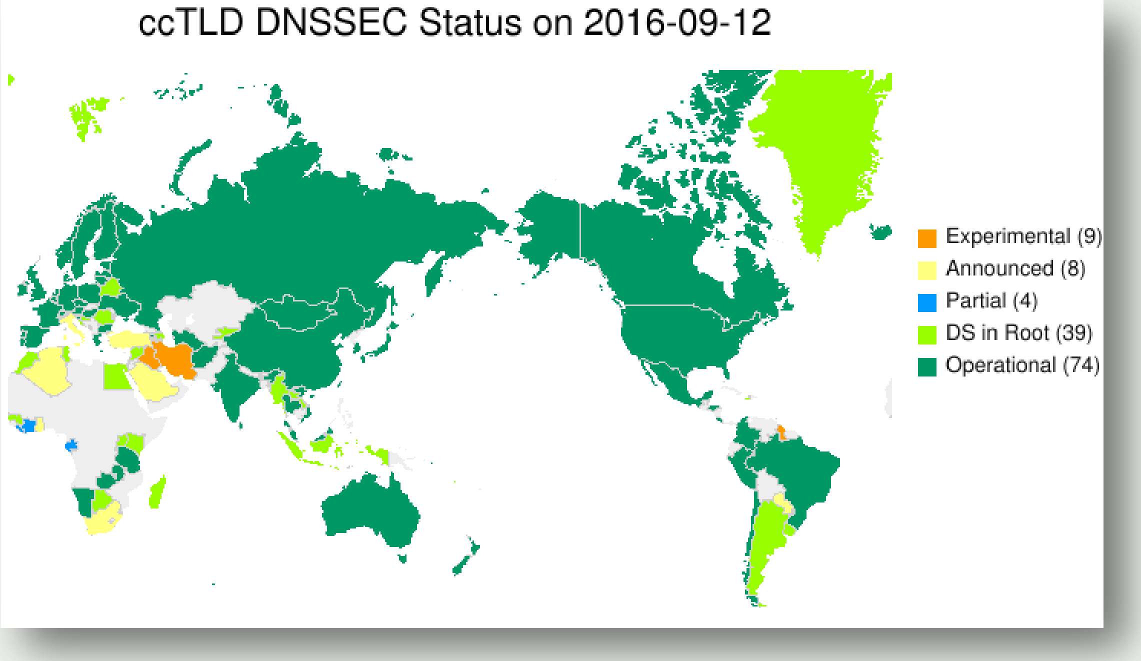
- Accepts DS records
- Sends DS to registry
- Provides UI for mgmt

- Signs zones
- Publishes all records
- Provides UI for mgmt

- Enables DNSSEC (unless automatic)

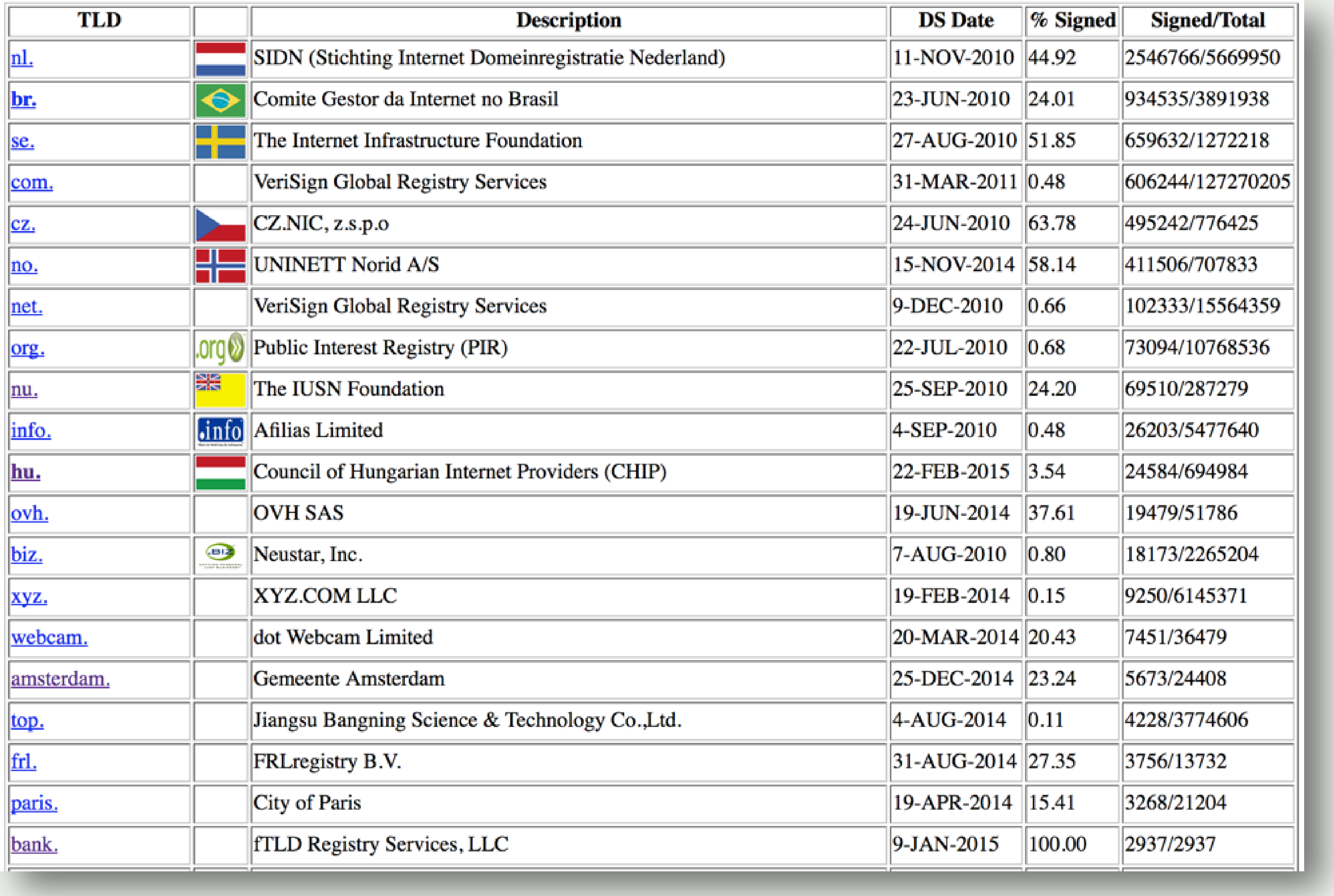
DNSSEC Signing – Current State

- Most TLDs now signed
  - including “new gTLDs”
- Common DNS servers all support DNSSEC
- Second-level domain support ranges from 100% in .BANK and 89% in .GOV down to < 1% in .COM
- Still small % overall.



https://www.internetsociety.org/deploy360/dnssec/maps/

DNSSEC Signing – Second-level domains



TLD		Description	DS Date	% Signed	Signed/Total
nl.		SIDN (Stichting Internet Domeinregistratie Nederland)	11-NOV-2010	44.92	2546766/5669950
br.		Comite Gestor da Internet no Brasil	23-JUN-2010	24.01	934535/3891938
se.		The Internet Infrastructure Foundation	27-AUG-2010	51.85	659632/1272218
com.		VeriSign Global Registry Services	31-MAR-2011	0.48	606244/127270205
cz.		CZ.NIC, z.s.p.o	24-JUN-2010	63.78	495242/776425
no.		UNINETT Norid A/S	15-NOV-2014	58.14	411506/707833
net.		VeriSign Global Registry Services	9-DEC-2010	0.66	102333/15564359
org.	.org	Public Interest Registry (PIR)	22-JUL-2010	0.68	73094/10768536
nu.		The IUSN Foundation	25-SEP-2010	24.20	69510/287279
info.	.info	Afilias Limited	4-SEP-2010	0.48	26203/5477640
hu.		Council of Hungarian Internet Providers (CHIP)	22-FEB-2015	3.54	24584/694984
ovh.		OVH SAS	19-JUN-2014	37.61	19479/51786
biz.		Neustar, Inc.	7-AUG-2010	0.80	18173/2265204
xyz.		XYZ.COM LLC	19-FEB-2014	0.15	9250/6145371
webcam.		dot Webcam Limited	20-MAR-2014	20.43	7451/36479
amsterdam.		Gemeente Amsterdam	25-DEC-2014	23.24	5673/24408
top.		Jiangsu Bangning Science & Technology Co.,Ltd.	4-AUG-2014	0.11	4228/3774606
frl.		FRLregistry B.V.	31-AUG-2014	27.35	3756/13732
paris.		City of Paris	19-APR-2014	15.41	3268/21204
bank.		fTLD Registry Services, LLC	9-JAN-2015	100.00	2937/2937

https://rick.eng.br/dnssecstat/

DNSSEC and TLS/SSL

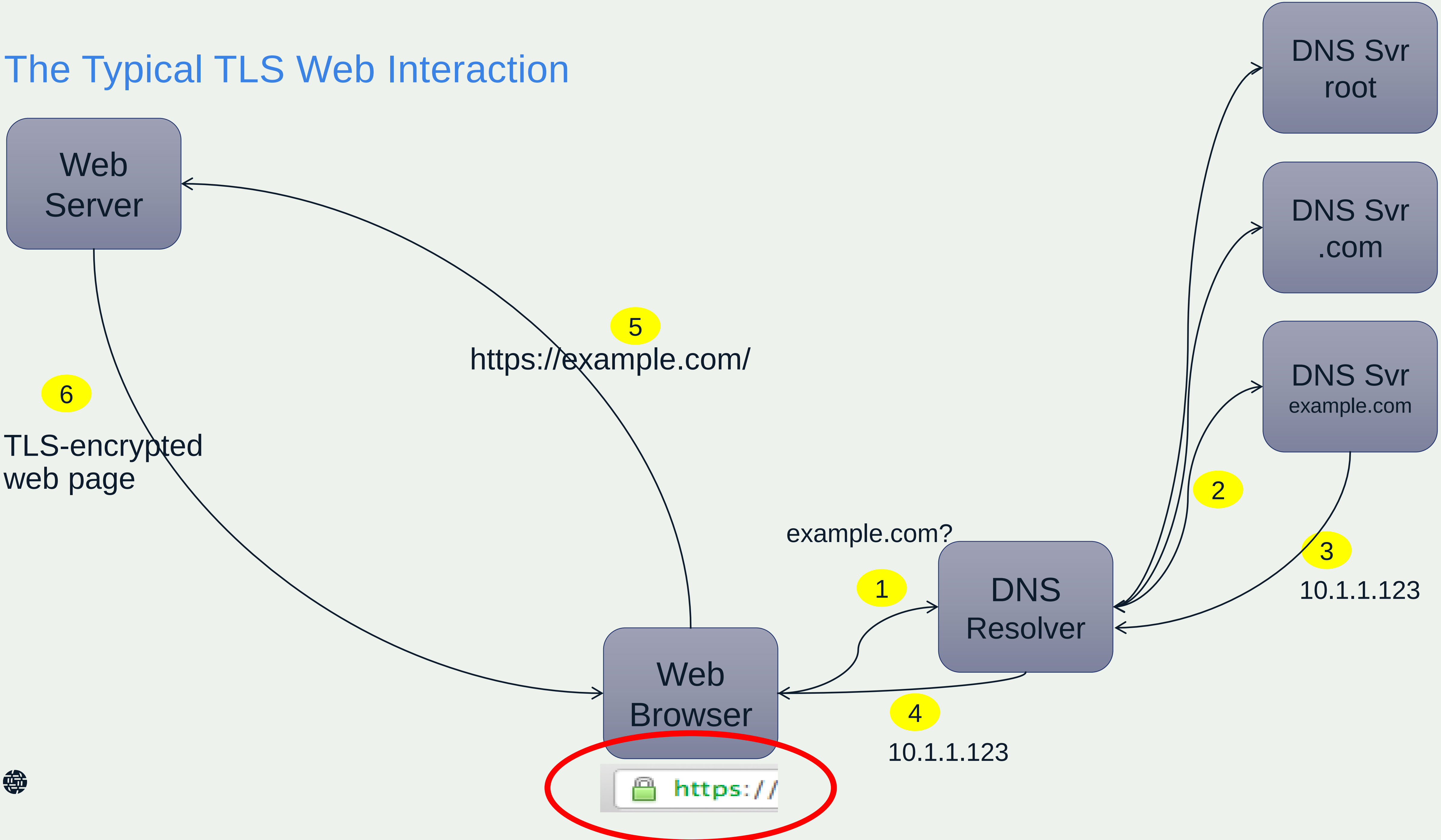
Why Do I Need DNSSEC If I Have TLS?

- A common question:

why do I need DNSSEC if I already have a SSL certificate? (or an "EV-SSL" certificate?)

- Transport Layer Security (TLS), sometimes called by its older name of “SSL”, solves a different issue – it provides encryption and protection of the communication between the browser and the web server

The Typical TLS Web Interaction



Web Server

DNS Svr root

DNS Svr .com

DNS Svr example.com

5 https://example.com/

6 TLS-encrypted web page

2

example.com?

3 10.1.1.123

1

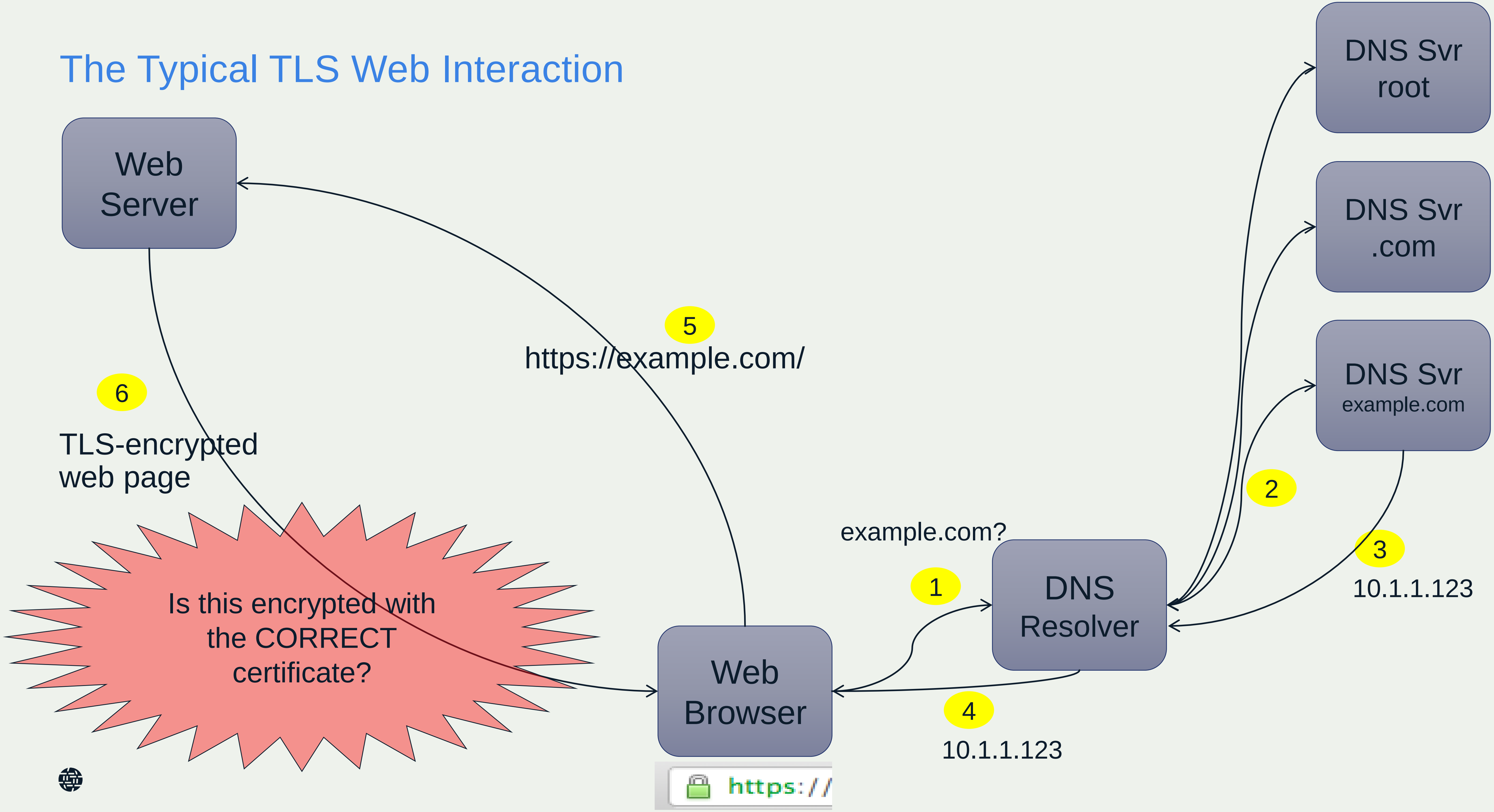
DNS Resolver

Web Browser

4 10.1.1.123

https://

The Typical TLS Web Interaction



DNS Svr
root

DNS Svr
.com

DNS Svr
example.com

Web
Server

5
https://example.com/

6
TLS-encrypted
web page

Is this encrypted with
the CORRECT
certificate?

2

example.com?

3
10.1.1.123

1

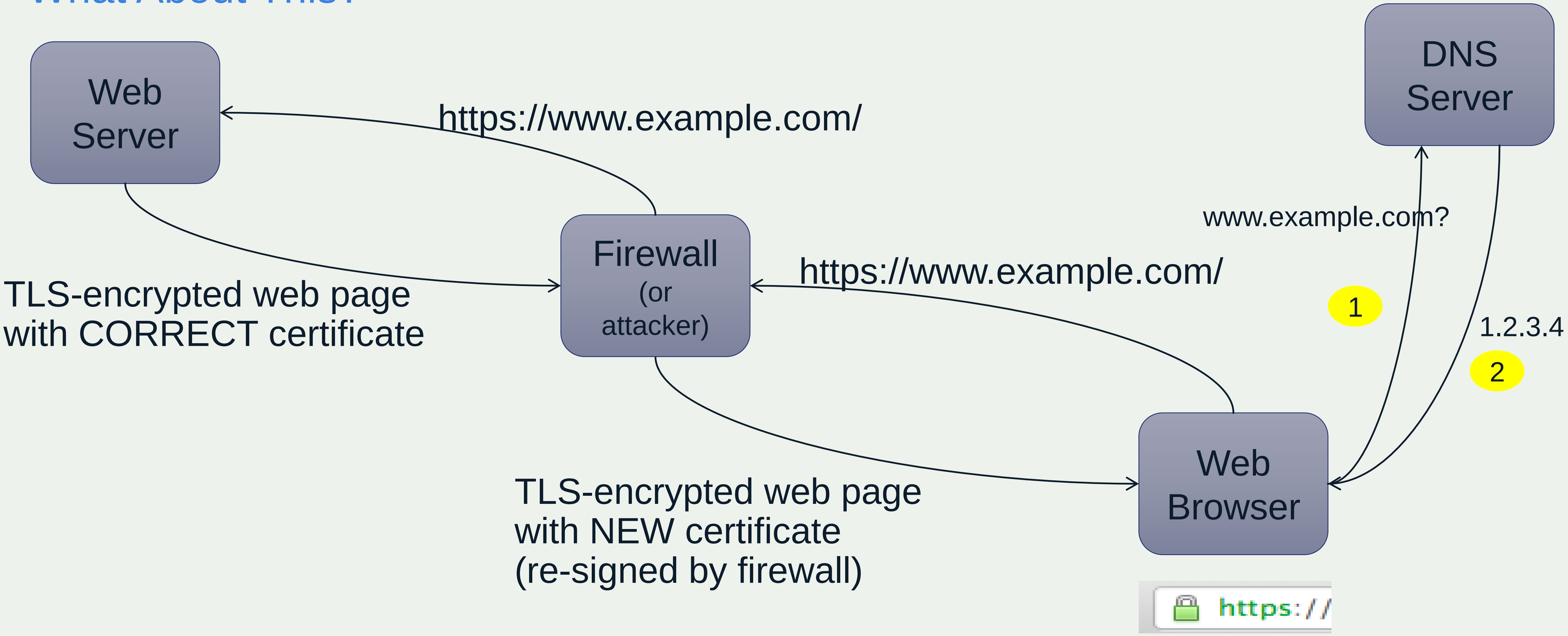
DNS
Resolver

Web
Browser

4
10.1.1.123

https://

What About This?



Web Server

https://www.example.com/

Firewall (or attacker)

DNS Server

www.example.com?

https://www.example.com/

1

1.2.3.4

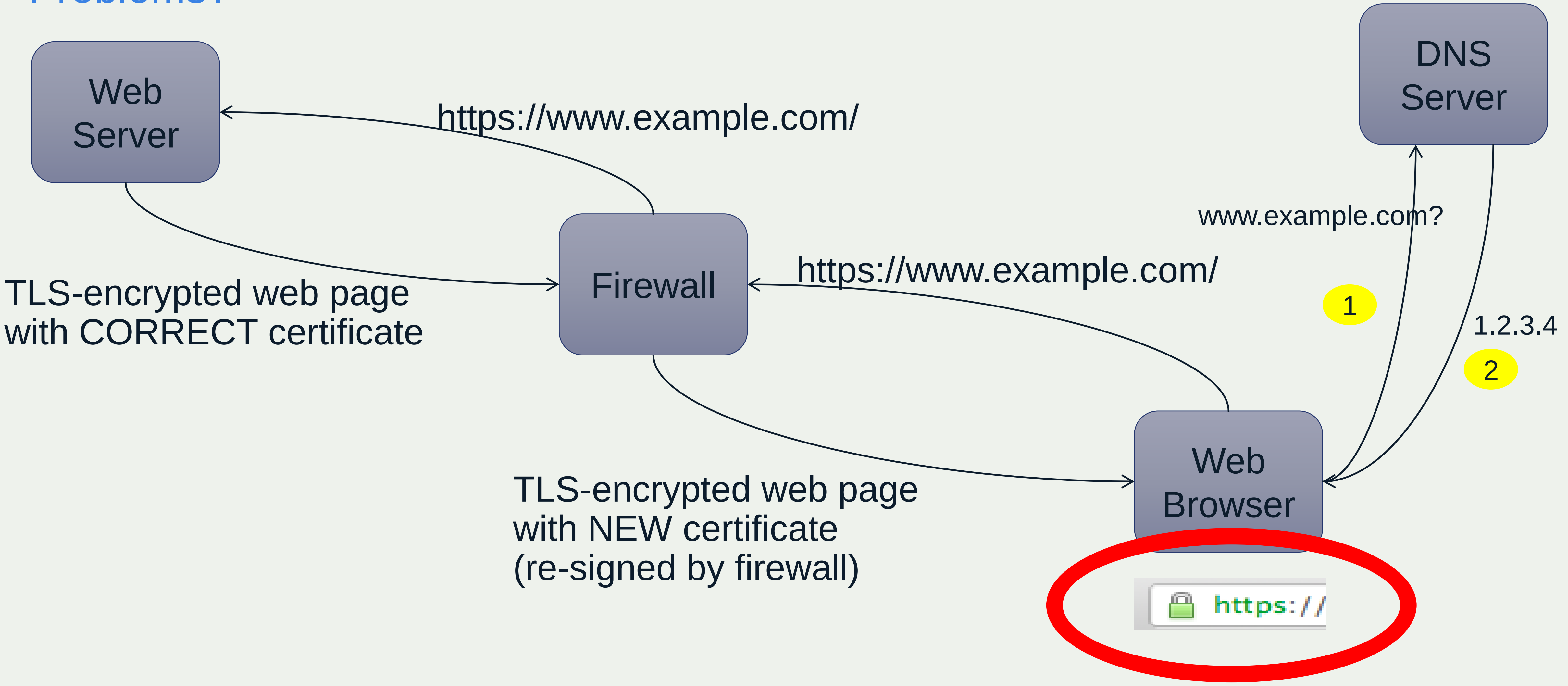
2

TLS-encrypted web page with CORRECT certificate

Web Browser

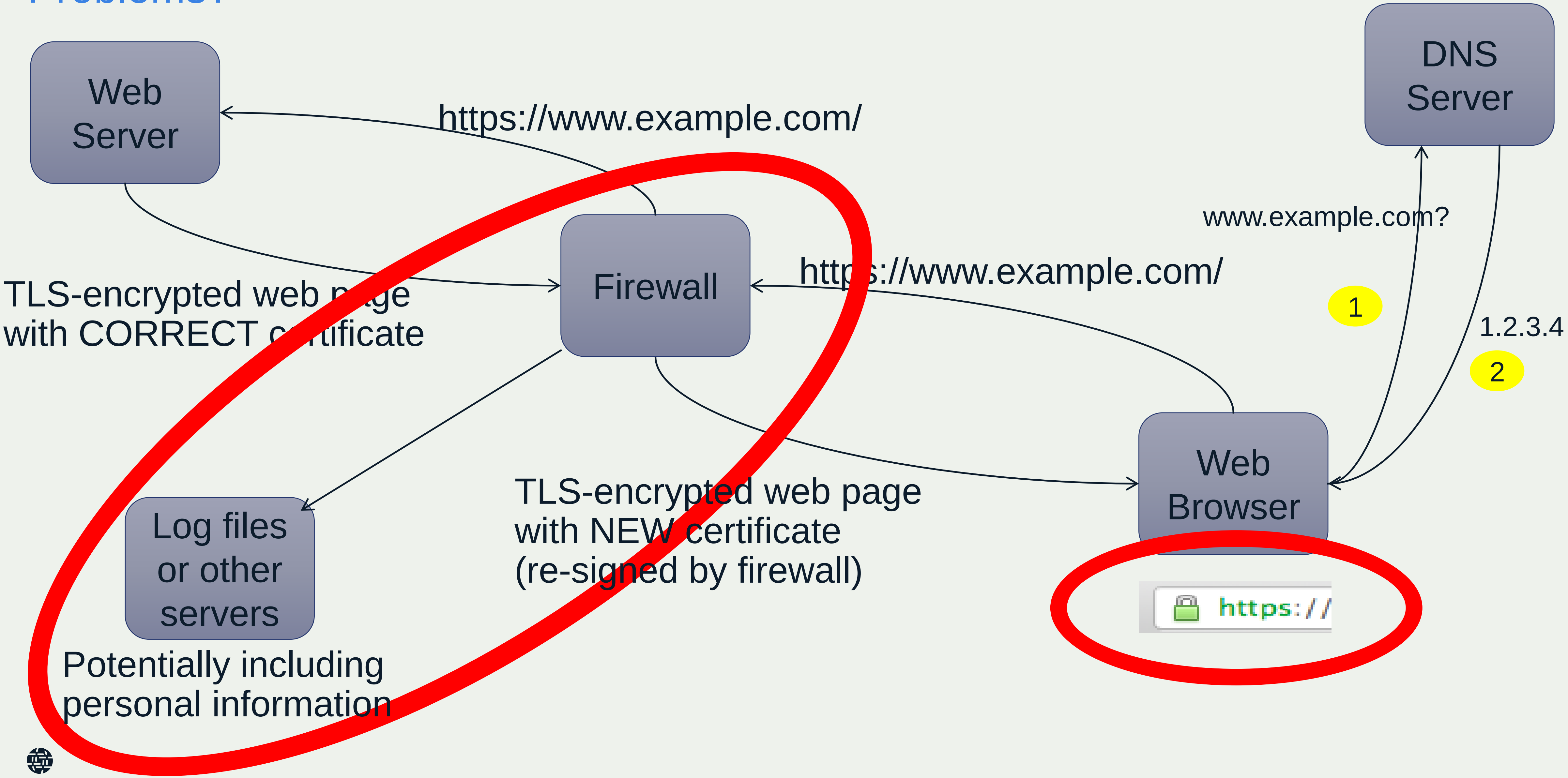
TLS-encrypted web page with NEW certificate (re-signed by firewall)

Problems?



Web Server
https://www.example.com/
DNS Server
www.example.com?
Firewall
https://www.example.com/
1
1.2.3.4
2
TLS-encrypted web page with CORRECT certificate
Web Browser
TLS-encrypted web page with NEW certificate (re-signed by firewall)
https://

Problems?



Web Server

https://www.example.com/

Firewall

TLS-encrypted web page with CORRECT certificate

Log files or other servers

Potentially including personal information

https://www.example.com/

TLS-encrypted web page with NEW certificate (re-signed by firewall)

DNS Server

www.example.com?

1

1.2.3.4

2

Web Browser

https://

Issues

- A Certificate Authority (CA) can sign ANY domain.
- Now over 1,500 CAs – there have been compromises where valid certs were issued for domains.
- Middle-boxes such as firewalls can re-sign sessions.

DNS-Based Authentication of Named Entities (DANE)

Q: How do you know if the TLS (SSL) certificate is the correct one the site wants you to use?
A: Store the certificate (or fingerprint) in DNS (new TLSA record) and sign them with DNSSEC.

An application that understand DNSSEC and DANE will then know when the required certificate is NOT being used.
Certificate stored in DNS is controlled by the domain name holder. It could be a certificate signed by a CA – or a self-signed certificate.

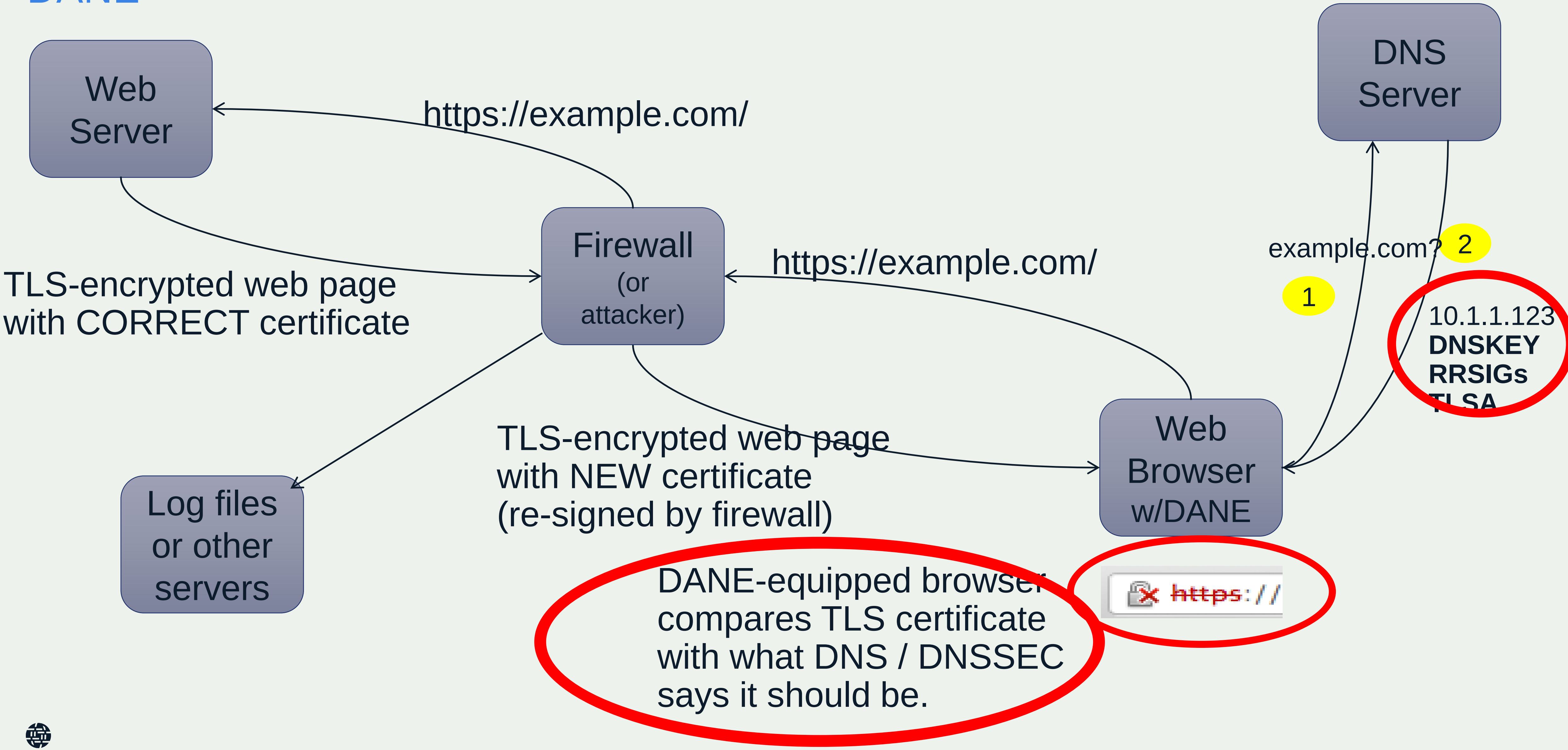
A Powerful Combination

- TLS = encryption + *limited* integrity protection
- DNSSEC = strong integrity protection

- How to get encryption + strong integrity protection?

- TLS + DNSSEC = DANE

DANE



TLS-encrypted web page with CORRECT certificate

TLS-encrypted web page with NEW certificate (re-signed by firewall)

DANE-equipped browser compares TLS certificate with what DNS / DNSSEC says it should be.

DANE Success – Not Just For The Web

SMTP

1000+ SMTP servers with TLSA records

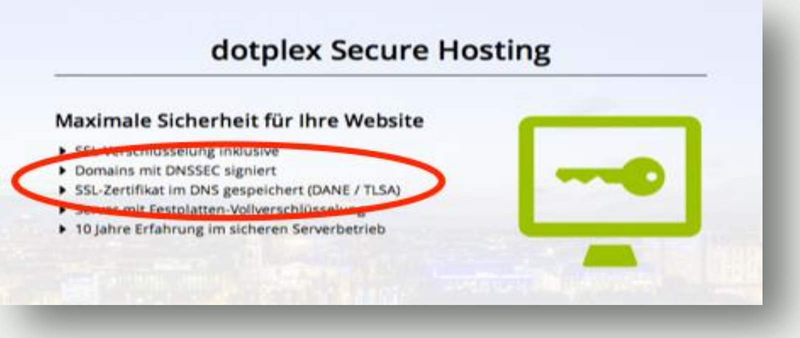
http://dane.sys4.de/ - testing service

XMPP (Jabber)

400+ servers

client-to-server & server-to-server

https://xmpp.net/reports.php#dnssecdane



dotplex Secure Hosting

Maximale Sicherheit für Ihre Website

- SSL-Verschlüsselung inklusive
- Domains mit DNSSEC signiert
- SSL-Zertifikat im DNS gespeichert (DANE / TLSA)
- Server mit Festplatten-Vollverschlüsselung
- 10 Jahre Erfahrung im sicheren Serverbetrieb

DANE Resources

DANE Overview and Resources:
    http://www.internetsociety.org/deploy360/resources/dane/

IETF Journal article explaining DANE:
    http://bit.ly/dane-dnssec

RFC 6394 - DANE Use Cases:
    http://tools.ietf.org/html/rfc6394

RFC 6698 – DANE Protocol:
    http://tools.ietf.org/html/rfc6698

DNS Privacy

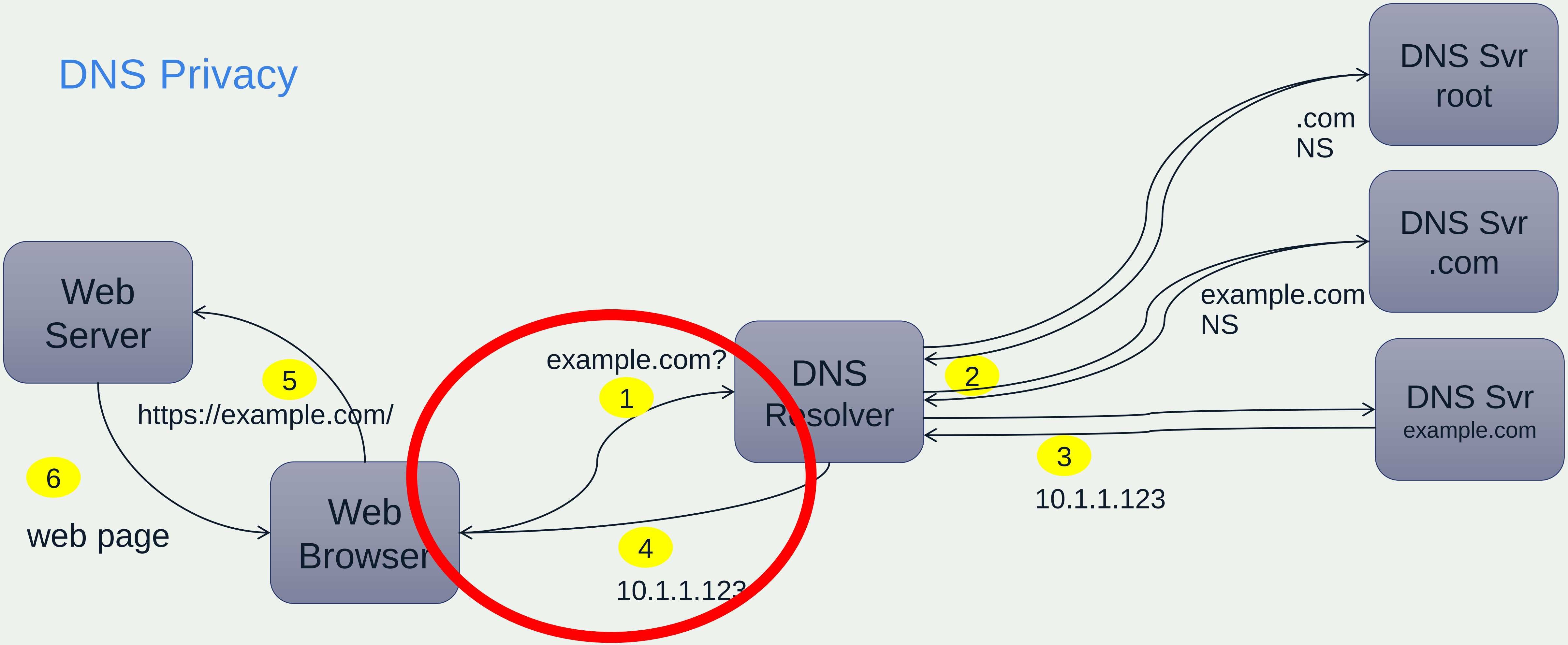
DNS Privacy

- Issue - Queries from local DNS “stub resolver” (in PC, laptop, smartphone) to local DNS resolver are sent in clear

- Surveillance of those queries can be revealing

- Solution – Encrypt the connection

DNS Privacy


DNS Svr
root
.com
NS
DNS Svr
.com
example.com
NS
Web
Server
5
https://example.com/
example.com?
1
DNS
Resolver
2
DNS Svr
example.com
6
web page
Web
Browser
4
10.1.1.123
3
10.1.1.123

DNS Privacy – Work Underway Now

- IETF “DPRIVE” Working Group
- New standards emerging– DNS queries over TLS
- Expect to see implementations in software and operating systems in the future

Business Reasons For Deploying DNSSEC

- TRUST – You can be sure your customers are reaching your sites – and that you are communicating with their servers.
- SECURITY – You can be sure you are communicating with the correct sites and not sharing business information with attackers, ex. email hijacking.
- INNOVATION – Services such as DANE built on top of DNSSEC enable innovative uses of TLS certificates.
- CONFIDENTIALITY – DANE enables easier use of encryption for applications and services that communicate across the Internet.

Three Requests For Attendees

1. Deploy DNSSEC validation (or ask your IT team / network operator)

1. Sign your domains
   - Work with your registrar and/or DNS hosting provider to make this happen.

2. Help promote support of DANE protocol
   - Let browser vendors and others know you want to use DANE. If you use SSL, deploy a TLSA record if you are able to do so. Help raise awareness of how DANE and DNSSEC can make the Internet more secure.

Thank you.

Dan York
Senior Content Strategist – york@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120