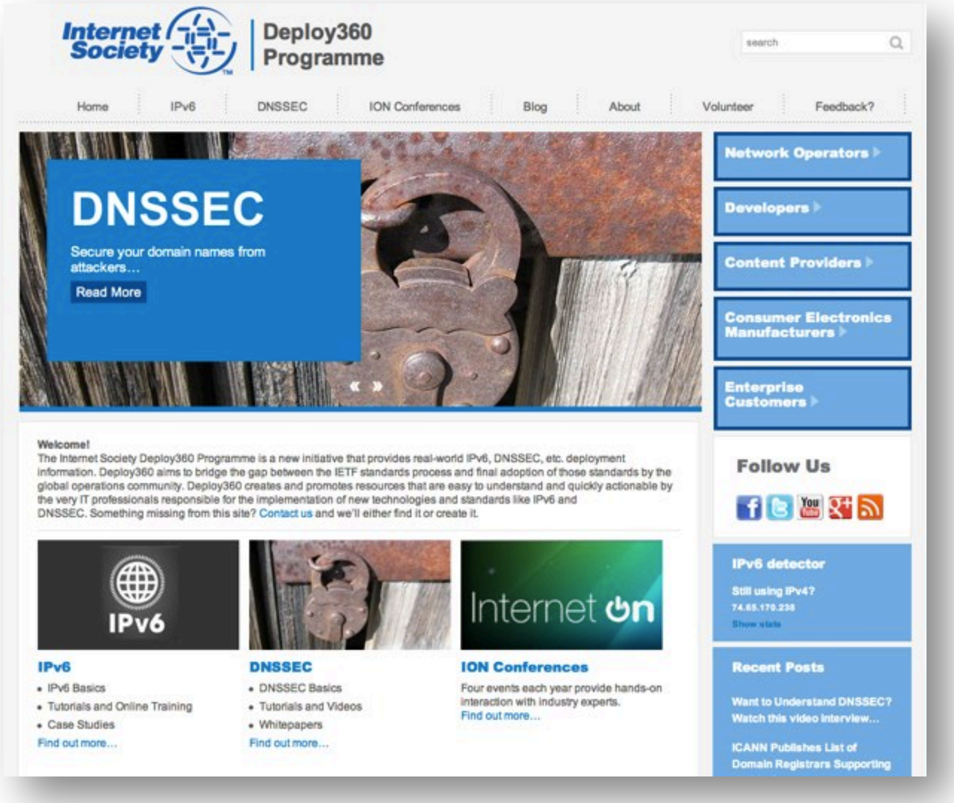
Next Steps In Accelerating DNSSEC Deployment

Dan York, CISSP
Senior Content Strategist, Internet Society

DNSSEC Deployment Workshop, ICANN 45
Toronto, Canada
October 17 , 2012

Internet Society Deploy360 Programme



DNSSEC

Secure your domain names from attackers...

Welcome!
The Internet Society Deploy360 Programme is a new initiative that provides real-world IPv6, DNSSEC, etc. deployment information. Deploy360 aims to bridge the gap between the IETF standards process and final adoption of those standards by the global operations community. Deploy360 creates and promotes resources that are easy to understand and quickly actionable by the very IT professionals responsible for the implementation of new technologies and standards like IPv6 and DNSSEC. Something missing from this site? Contact us and we'll either find it or create it.

IPv6
- IPv6 Basics
- Tutorials and Online Training
- Case Studies

Find out more...

DNSSEC
- DNSSEC Basics
- Tutorials and Videos
- Whitepapers

Find out more...

ION Conferences
Four events each year provide hands-on interaction with industry experts.
Find out more...

IPv6 detector
Still using IPv4?
74.65.170.236
Show stats

Recent Posts

Want to Understand DNSSEC? Watch this video interview...

ICANN Publishes List of Domain Registrars Supporting

www.internetsociety.org/deploy360/

Providing real-world deployment info for IPv6, DNSSEC and other Internet technologies:

- **Case Studies**
- **Tutorials**
- **Videos**
- **Whitepapers**
- **News, information**

English content, initially, but will be translated into other languages.

Key Questions

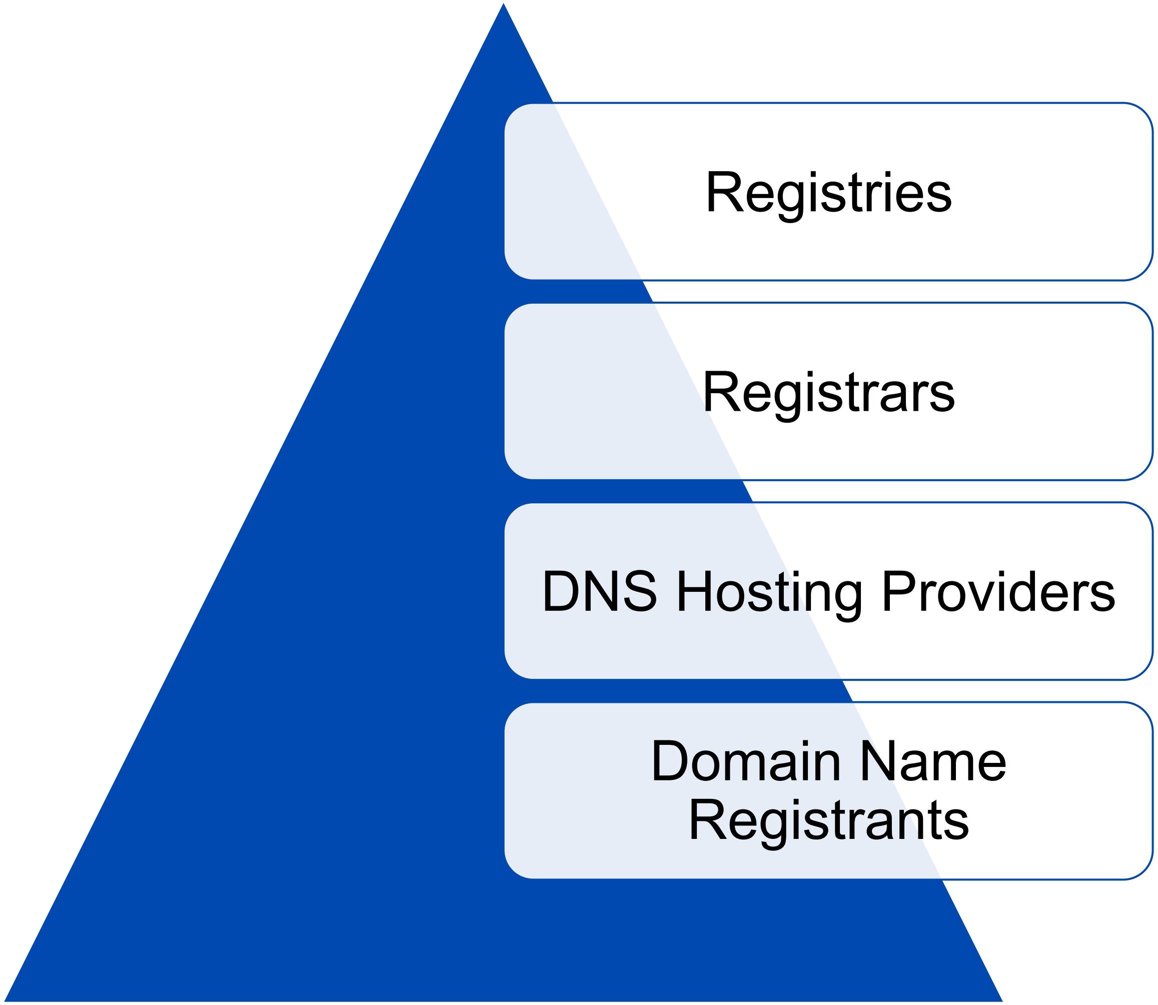
- What needs to be done to get more domains signed with DNSSEC?
- How can DNSSEC validation be more widely deployed?
- Are there technical issues or are the issues more of communication and awareness?
- How can we as a community address these challenges to increase the usage and availability of DNSSEC?

Opportunities to Accelerate Deployment

1. **Registrar / DNS hosting provider engagement**
   - Encouraging more registrars to provide DNSSEC and making it easier for domain name holders.
2. **Validating name servers**
   - Expanding the deployment of DNSSEC-validating name servers at multiple levels, including ISPs, operating systems and applications.
3. **Enterprise signing of domains**
   - Helping enterprises and other large organizations understand the added security value they can achieve with DNSSEC, particularly with the new capabilities of DANE.
4. **Government activity with DNSSEC**
   - Encouraging governments to expand their promotion and usage of DNSSEC

Registries / Registrars / DNS Hosting Providers

DNSSEC Signing - The Players



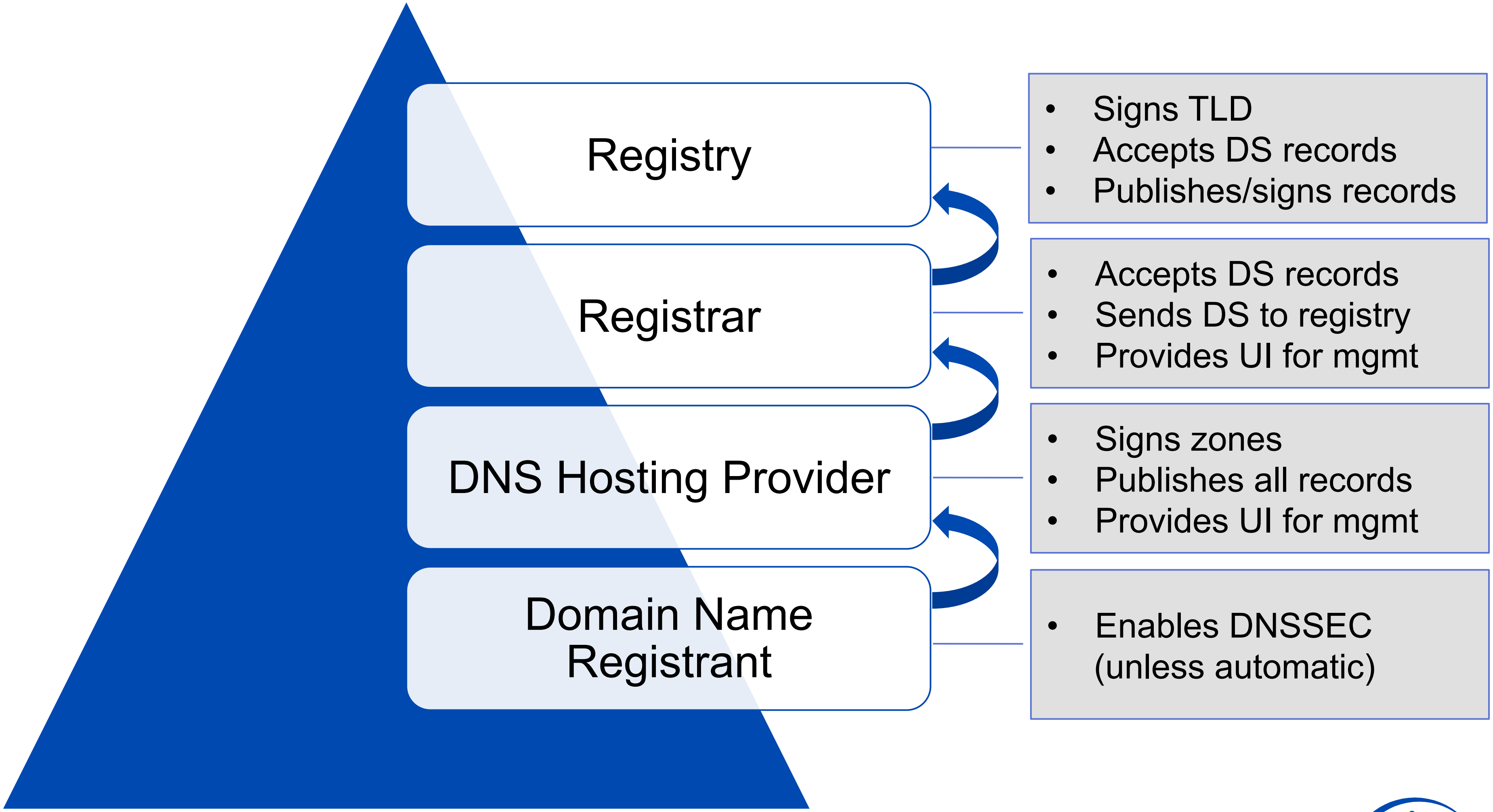
Registries

Registrars

DNS Hosting Providers

Domain Name Registrants

DNSSEC Signing - The Individual Steps



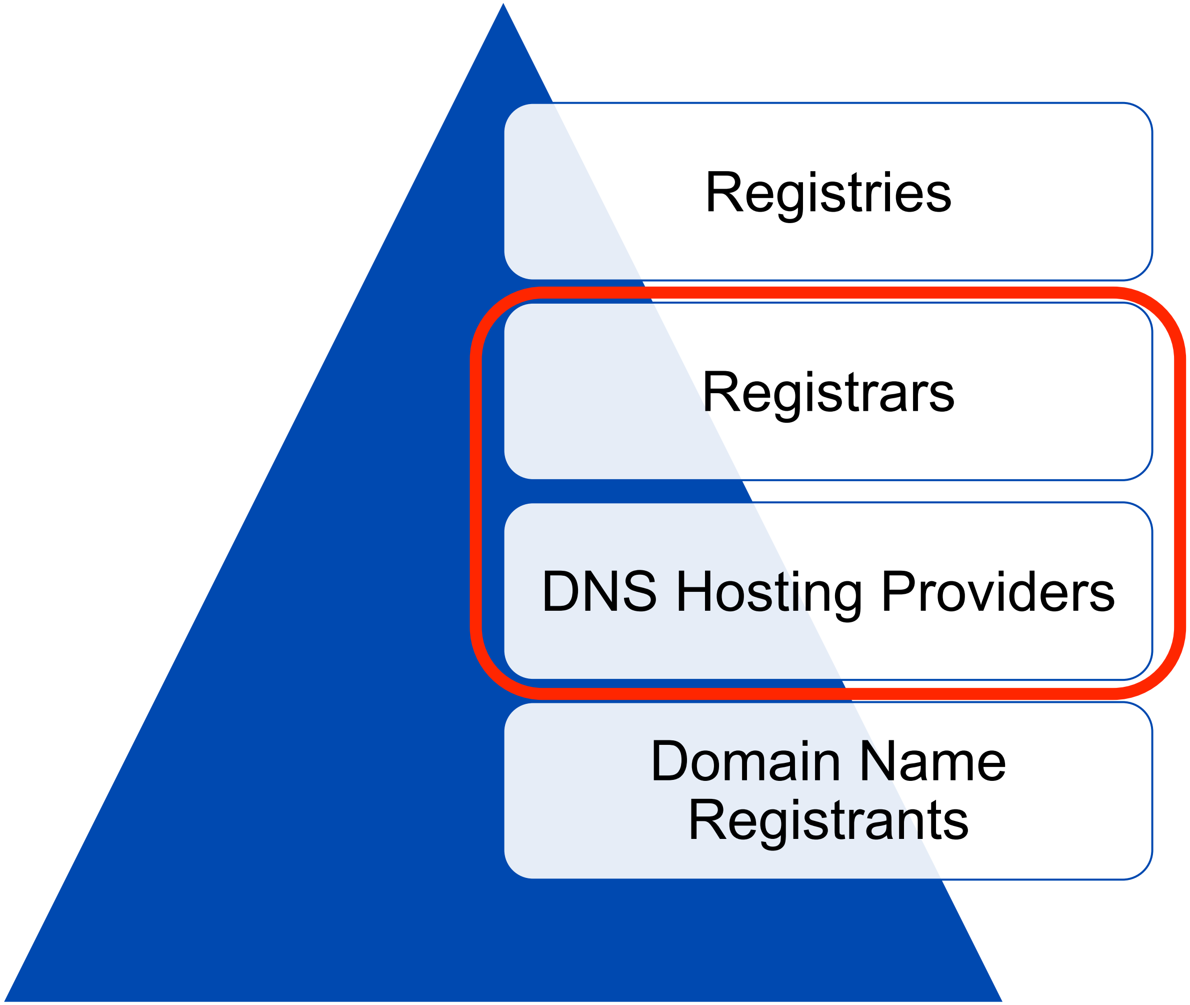
- Signs TLD
- Accepts DS records
- Publishes/signs records

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

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

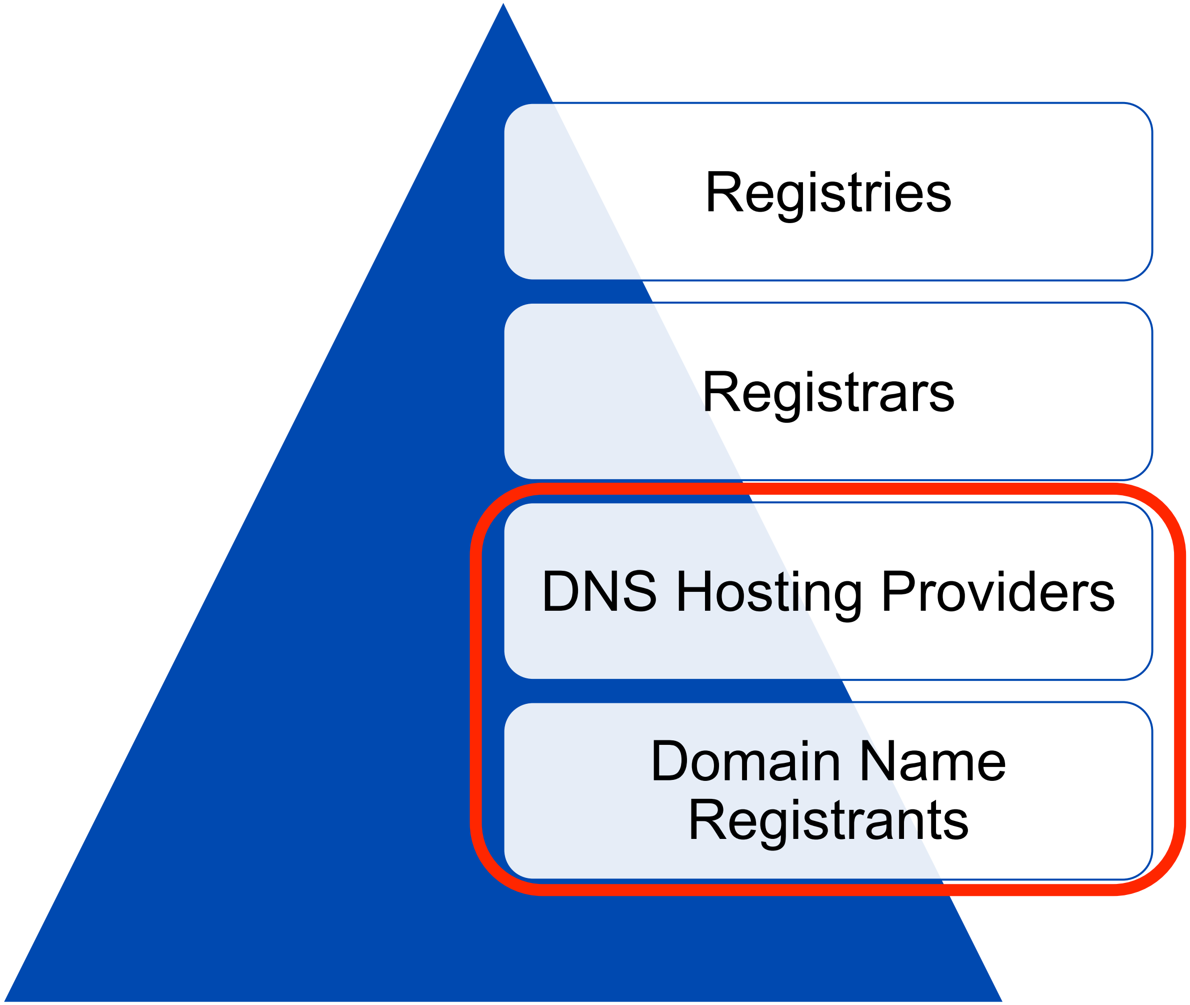
- Enables DNSSEC (unless automatic)

DNSSEC Signing - The Players



Registrar also provides DNS hosting services

DNSSEC Signing - The Players



Registries

Registrars

DNS Hosting Providers

Domain Name Registrants

Registrant hosts own DNS

Three General Points:

1. **Registries** need to make it as simple as possible for registrars to upload Delegation Signer (DS) records

2. **Registrars** need to make it as simple as possible for DNS hosting providers (including domain name registrants who self-host their DNS) to upload DS records

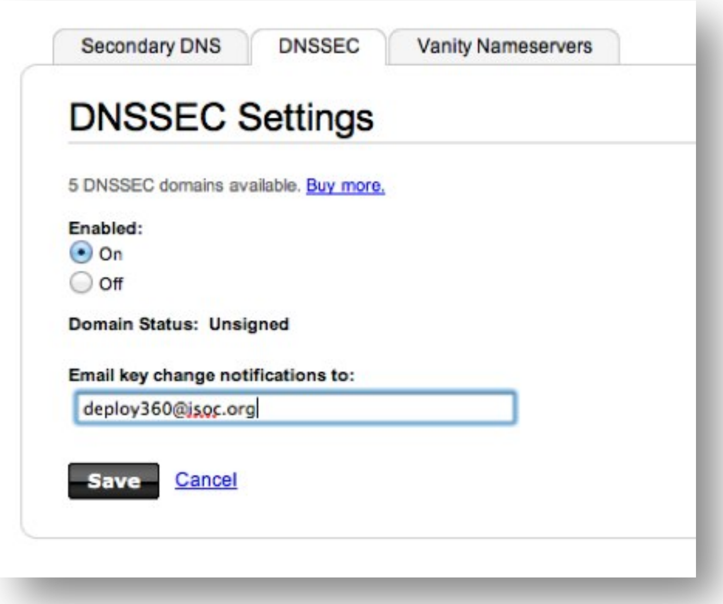
3. **DNS hosting providers** need to make it as simple - and as automated - as possible for domain name registrants to sign domains

Note: If you are not aware, a DS record ties the DNSSEC-signed DNS zone into the global "chain of trust".

Simplify The Registrar/Hosting Experience

We need to make the DNSSEC-signing process at domain name registrars *easy* for *domain name registrants / holders*. Examples:

- Binero in Sweden signs all domains by default
- GoDaddy provides a "one-click" button as part of "Premium DNS" offering
- All keys automatically generated and handled for the domain name holder



DNSSEC Settings

5 DNSSEC domains available. Buy more.

Enabled:
● On
○ Off

Domain Status: Unsigned

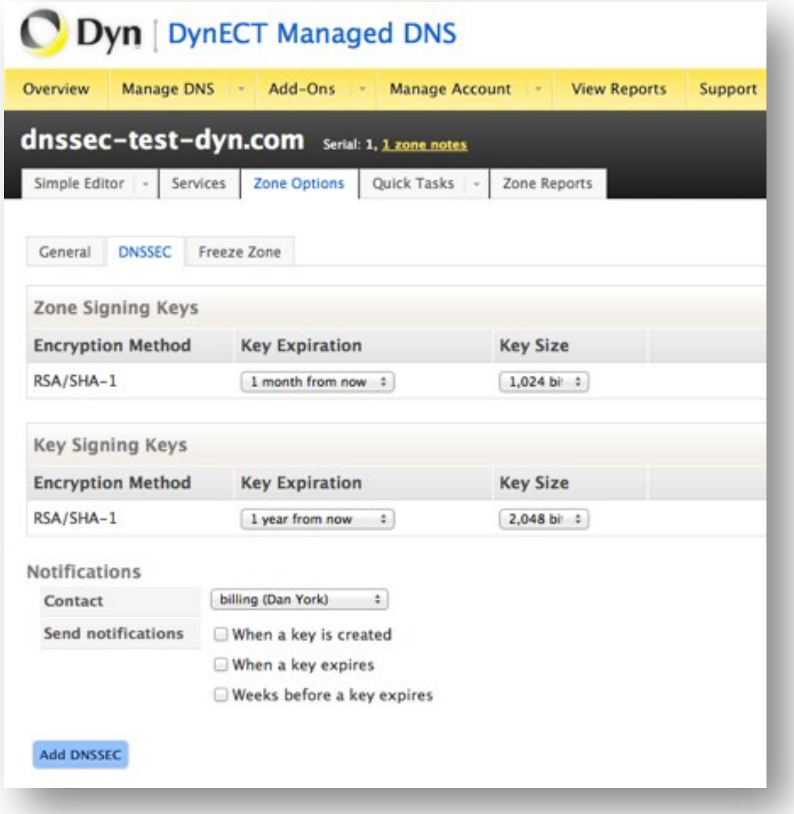
Email key change notifications to:
deploy360@isoc.org

Simplify The DNS Hosting Experience

Another example, Dyn, Inc:

- Provides a simple experience – just click “Add DNSSEC” at the bottom
- Availability of options may be good for technical users but confusing / intimidating for new users

Need this kind of simple interface at more DNS hosting providers



dnssec-test-dyn.com Serial: 1, 1 zone notes

Zone Signing Keys

Encryption Method	Key Expiration	Key Size
RSA/SHA-1	1 month from now	1,024 bi

Key Signing Keys

Encryption Method	Key Expiration	Key Size
RSA/SHA-1	1 year from now	2,048 bi

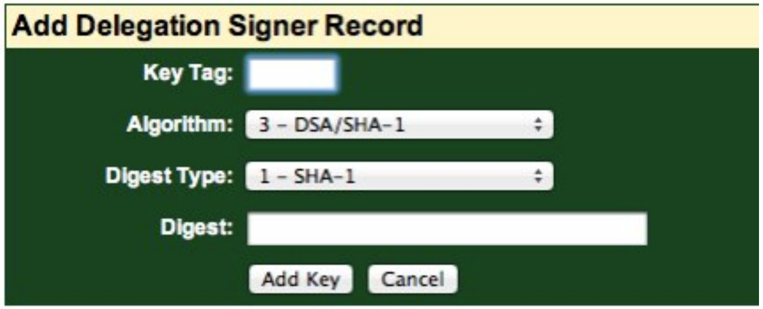
Notifications

Contact: billing (Dan York)

Send notifications:
□ When a key is created
□ When a key expires
□ Weeks before a key expires

Simplify/Automate Transfer of DS Records

If DNS is hosted with one provider (including self-hosted), process of getting Delegation Signer (DS) record to registrar is primarily copy / paste between web forms.



Add Delegation Signer Record

Key Tag:

Algorithm: 3 - DSA/SHA-1

Digest Type: 1 - SHA-1

Digest:

- Ideally needs to be automated to remove this extra step

Some registrars offering API. Example:

- www.gkg.net/ws/ds.html

Registrars / DNS Hosting Providers

Two technical issues:

- **REGISTRAR TO REGISTRY**
  - Upload of DS records
  - Multiple DS records (to support key rollover)
  - Use of EPP?
- **DNS HOSTING PROVIDER TO REGISTRAR**
  - Upload of DS records
  - No standardized API – mainly propriety APIs or web UI copy/paste

Increase Number of Domain Name Registrars

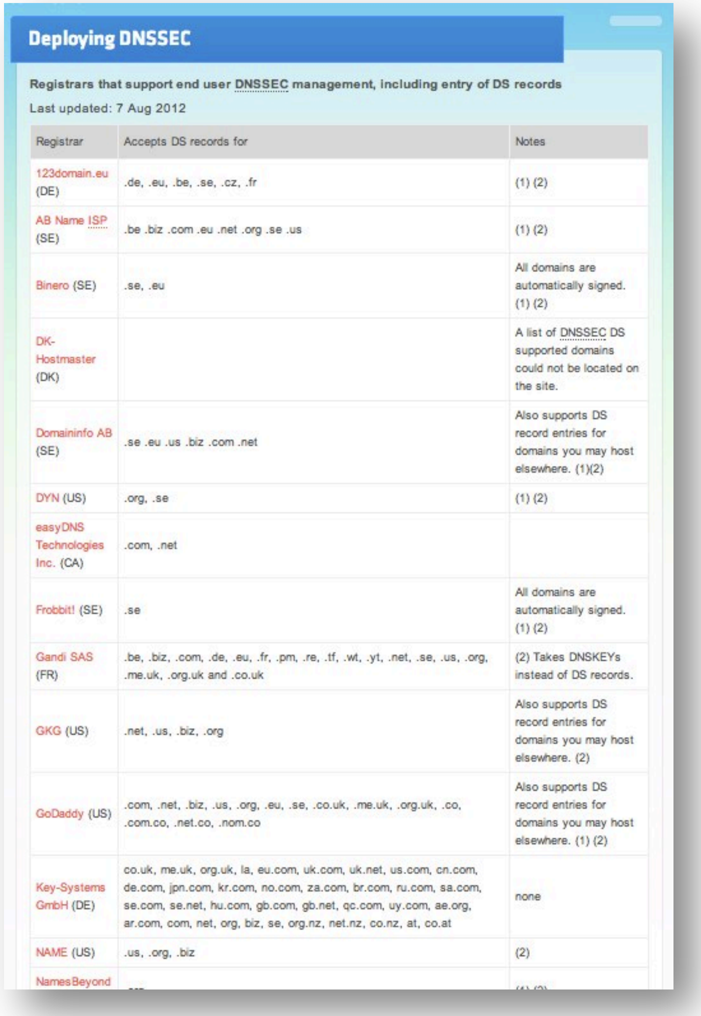
Need to increase number of domain name registrars supporting DNSSEC

- Good news is that the list keeps increasing!

List from ICANN at:

- www.icann.org/en/news/in-focus/dnssec/deployment

If you are a registar and support DNSSEC, you can ask to be added to ICANN's list.



Registrars that support end user DNSSEC management, including entry of DS records

Last updated: 7 Aug 2012

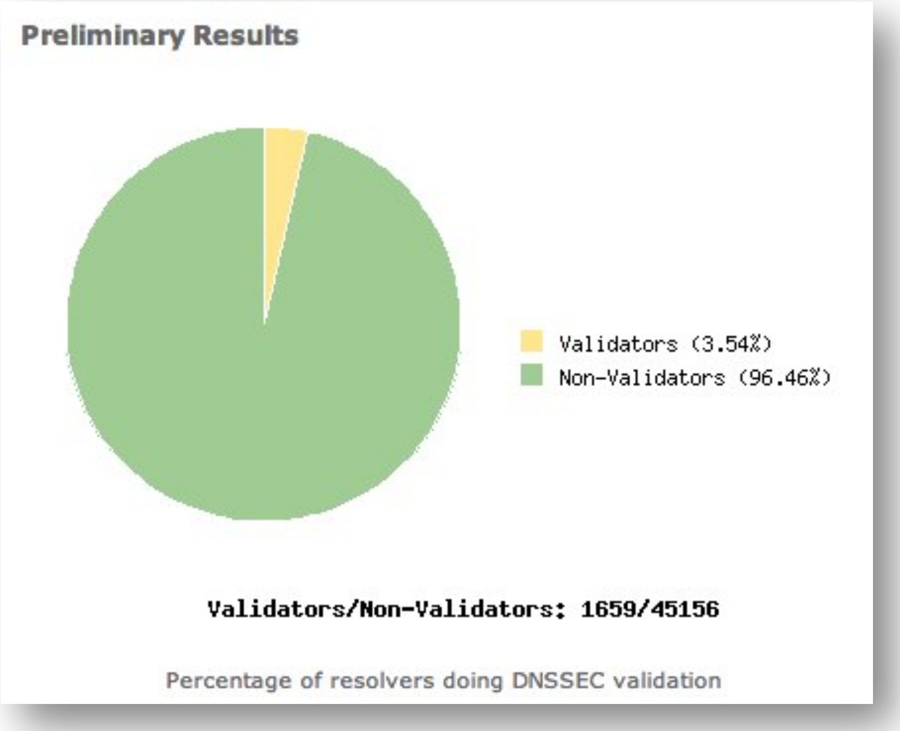
Registrar	Accepts DS records for	Notes
123domain.eu (DE)	.de, .eu, .be, .se, .cz, .fr	(1) (2)
AB Name ISP (SE)	.be .biz .com .eu .net .org .se .us	(1) (2)
Binero (SE)	.se, .eu	All domains are automatically signed. (1) (2)
DK-Hostmaster (DK)		A list of DNSSEC DS supported domains could not be located on the site.
Domaininfo AB (SE)	.se .eu .us .biz .com .net	Also supports DS record entries for domains you may host elsewhere. (1)(2)
DYN (US)	.org, .se	(1) (2)
easyDNS Technologies Inc. (CA)	.com, .net	
Frobbit! (SE)	.se	All domains are automatically signed. (1) (2)
Gandi SAS (FR)	.be, .biz, .com, .de, .eu, .fr, .pm, .re, .tf, .wt, .yt, .net, .se, .us, .org, .me.uk, .org.uk and .co.uk	(2) Takes DNSKEYs instead of DS records.
GKG (US)	.net, .us, .biz, .org	Also supports DS record entries for domains you may host elsewhere. (2)
GoDaddy (US)	.com, .net, .biz, .us, .org, .eu, .se, .co.uk, .me.uk, .org.uk, .co, .com.co, .net.co, .nom.co	Also supports DS record entries for domains you may host elsewhere. (1) (2)
Key-Systems GmbH (DE)	co.uk, me.uk, org.uk, la, eu.com, uk.com, uk.net, us.com, cn.com, de.com, jpn.com, kr.com, no.com, za.com, br.com, ru.com, sa.com, se.com, se.net, hu.com, gb.com, gb.net, qc.com, uy.com, ae.org, ar.com, com, net, org, biz, se, org.nz, net.nz, co.nz, at, co.at	none
NAME (US)	.us, .org, .biz	(2)
NamesBeyond		

Source: www.icann.org/en/news/in-focus/dnssec/deployment

Validating Name Servers

Validating Name Servers

- **How do we increase the percentage?**



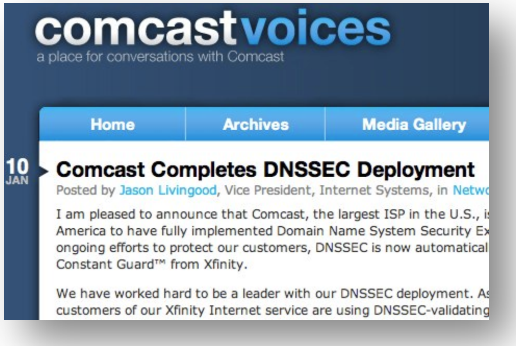
Validators/Non-Validators: 1659/45156

Percentage of resolvers doing DNSSEC validation

http://validator-search.verisignlabs.com

Availability of DNSSEC-Validating Resolvers

Consumers need easy availability of DNSSEC-validating DNS resolvers. Examples:



Comcast Completes DNSSEC Deployment

Posted by Jason Livingood, Vice President, Internet Systems, in Netwo

I am pleased to announce that Comcast, the largest ISP in the U.S., is
America to have fully implemented Domain Name System Security Ex
ongoing efforts to protect our customers, DNSSEC is now automatical
Constant Guard™ from Xfinity.

We have worked hard to be a leader with our DNSSEC deployment. As
customers of our Xfinity Internet service are using DNSSEC-validating

- Comcast in North America recently rolled out DNSSEC-validating resolvers to 18+ million customers

- Almost all ISPs in Sweden and Czech Republic provide DNSSEC-validating resolvers

Validating Name Servers – How To Get There

- Education about value in DNSSEC validation
- Requests from customer base (i.e. larger education)
- Education about available tools and better automation within tools wherever possible
- More case studies, tutorials

Enterprises / Domain Name Holders

Key Steps for Enterprises / Governments

Steps:

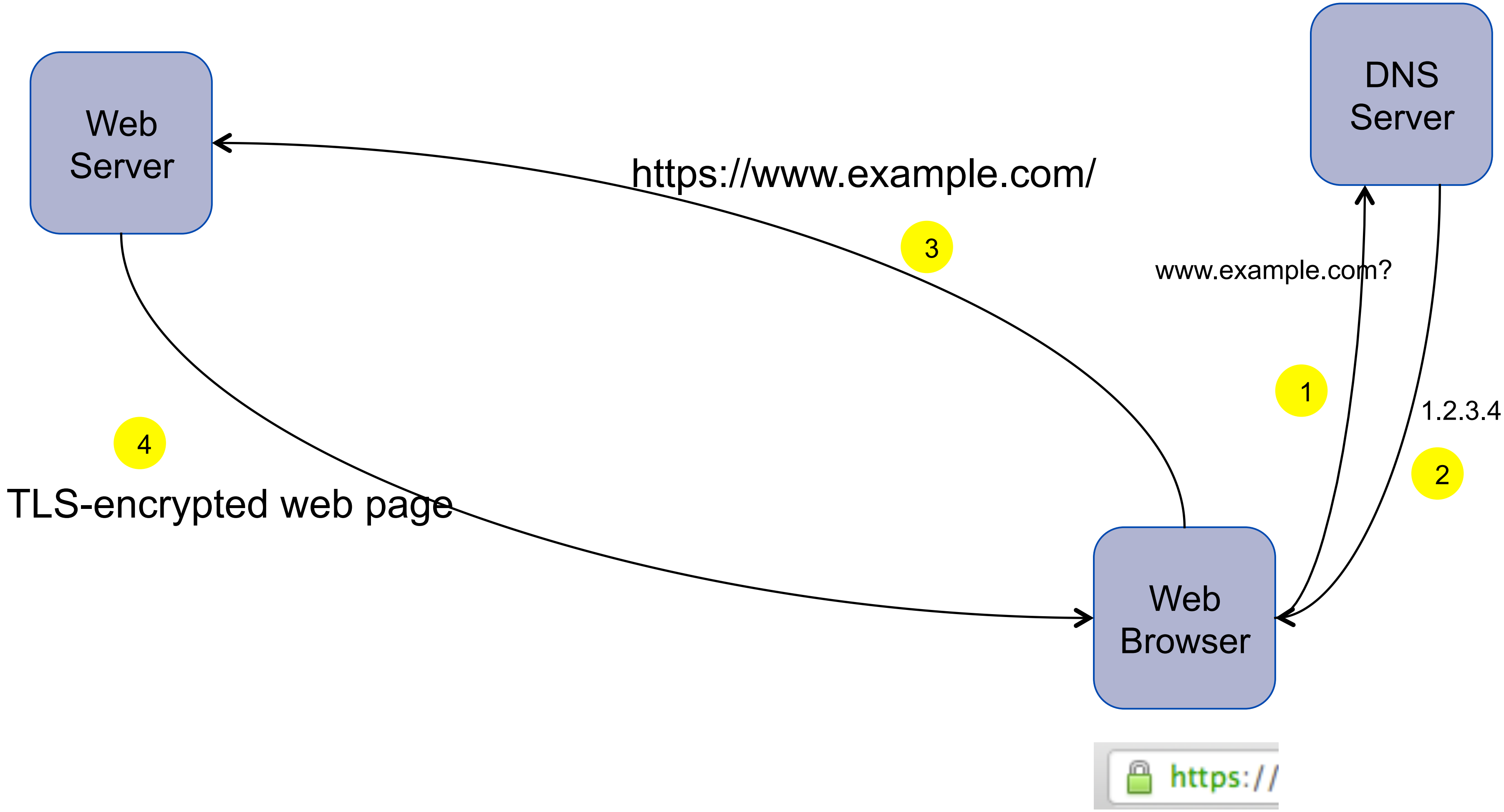
1. Sign domain(s)
2. Enable/install DNSSEC-validating name servers

Needed:

- Simplification of registrar / DNS hosting experience
- Education about basics of DNSSEC and the value
- More articles in mainstream IT media, more presentations at IT conferences
- More tutorials, more tools
- DANE…

DANE

The Typical TLS (SSL) Web Interaction



Web Server

DNS Server

https://www.example.com/

3

www.example.com?

1

1.2.3.4

2

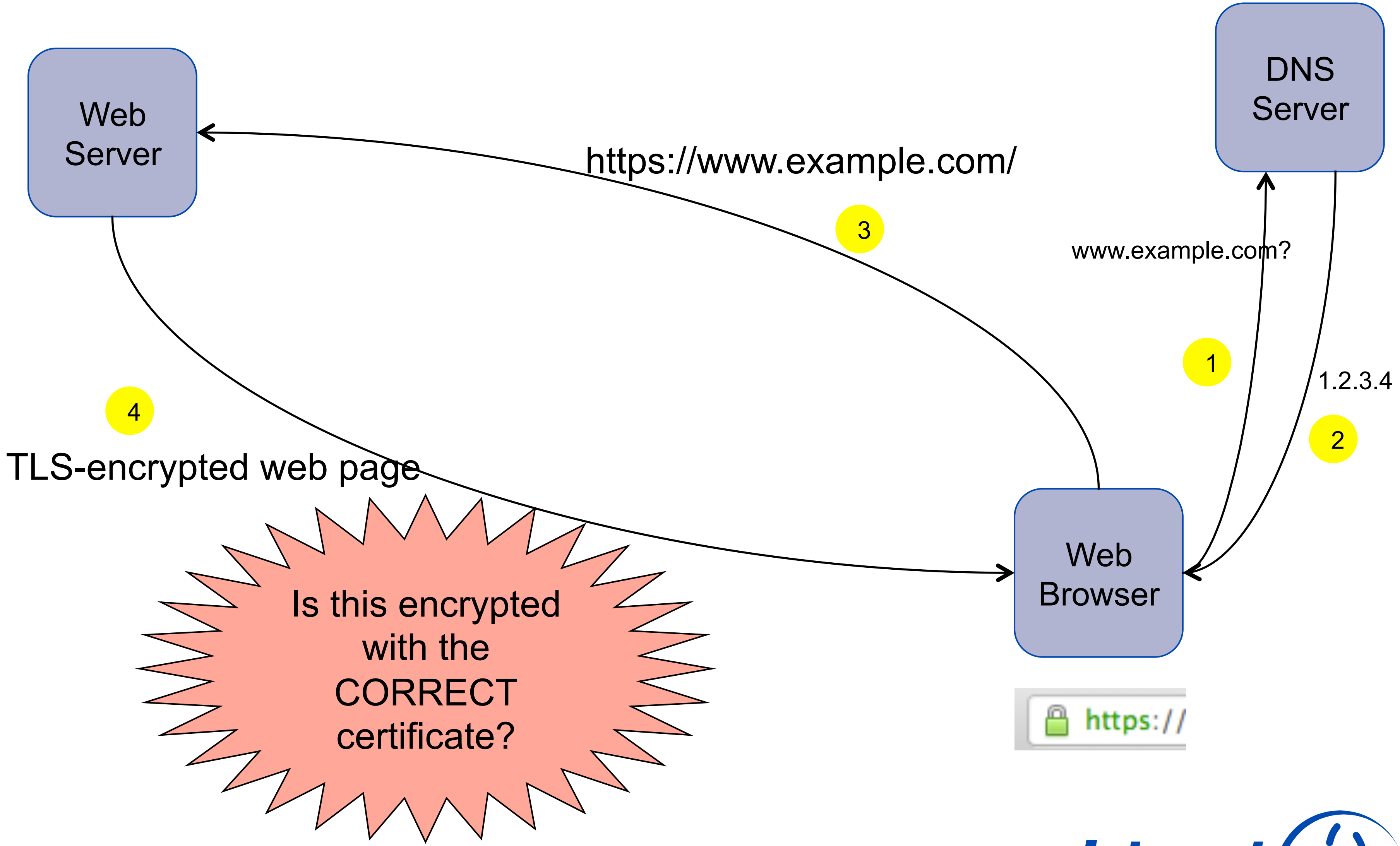
4

TLS-encrypted web page

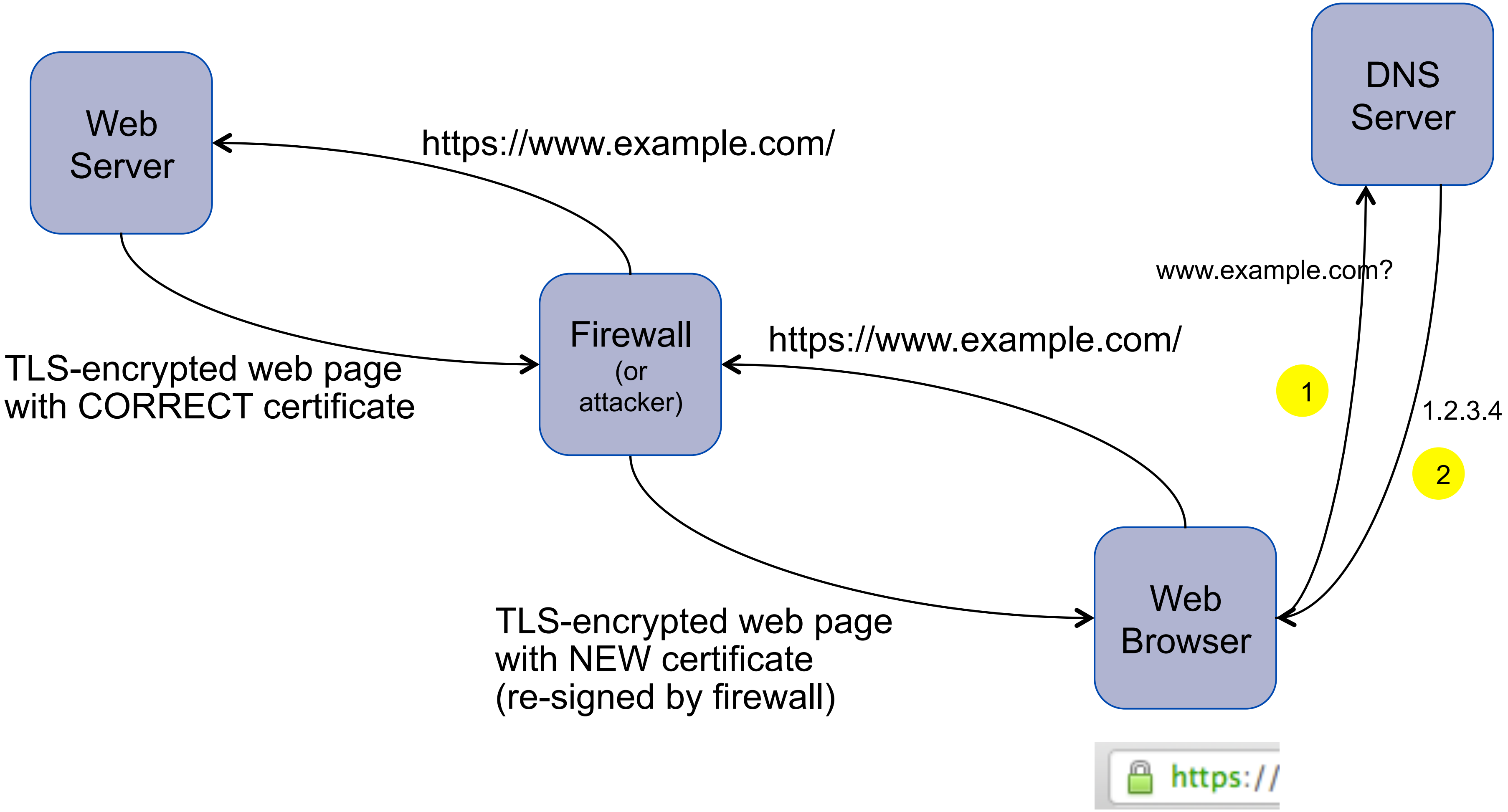
Web Browser

https://

The Typical TLS (SSL) Web Interaction



What About This?



Web Server

https://www.example.com/

TLS-encrypted web page with CORRECT certificate

Firewall (or attacker)

https://www.example.com/

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

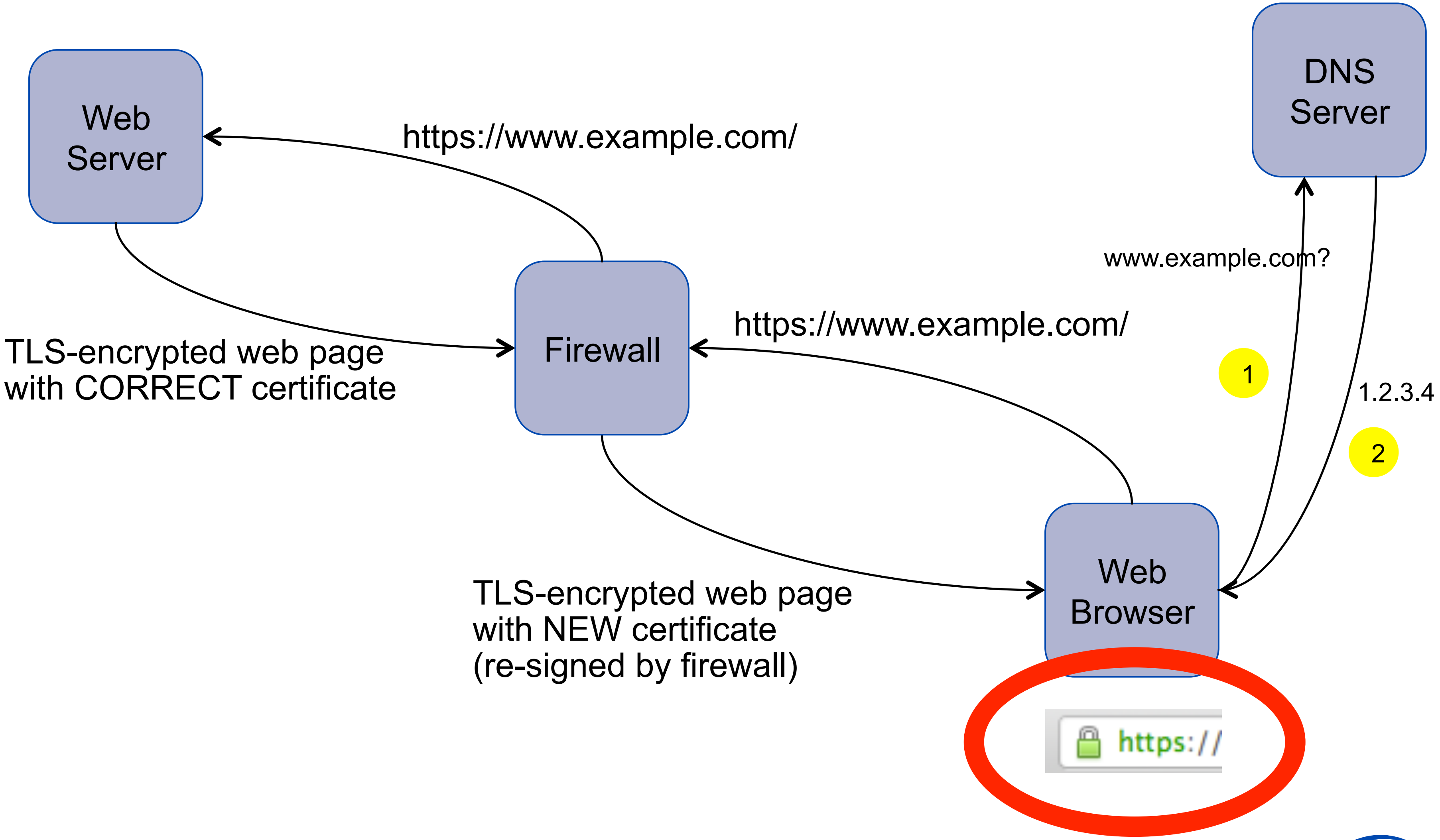
DNS Server

www.example.com?

1.2.3.4

Web Browser

Problems?



Web Server

https://www.example.com/

Firewall

TLS-encrypted web page
with CORRECT certificate

DNS Server

www.example.com?

https://www.example.com/

1

1.2.3.4

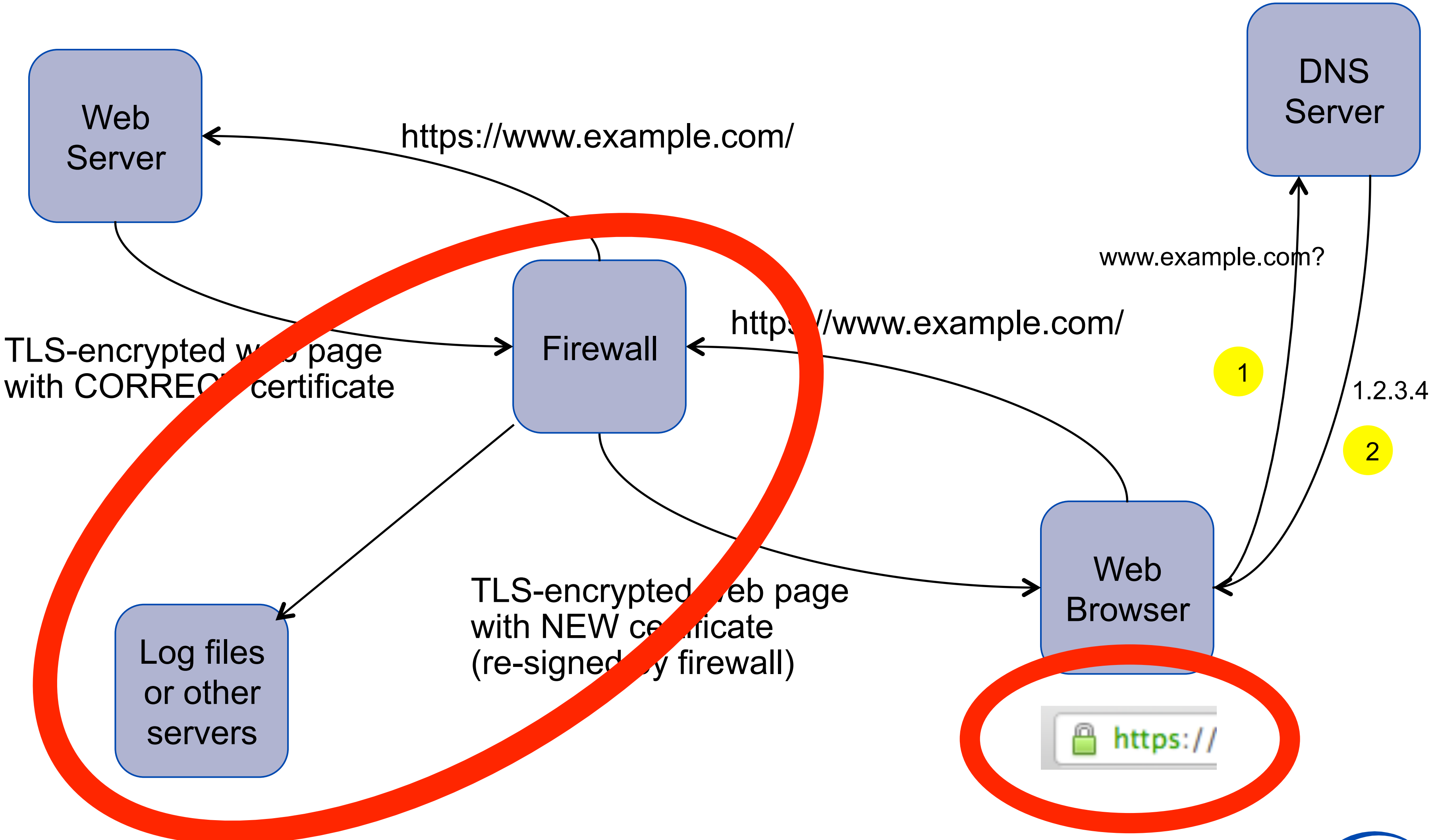
2

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

https://www.example.com/

DNS Server

www.example.com?

1

1.2.3.4

2

Log files or other servers

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

Web Browser

https://

Potentially including personal information

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)

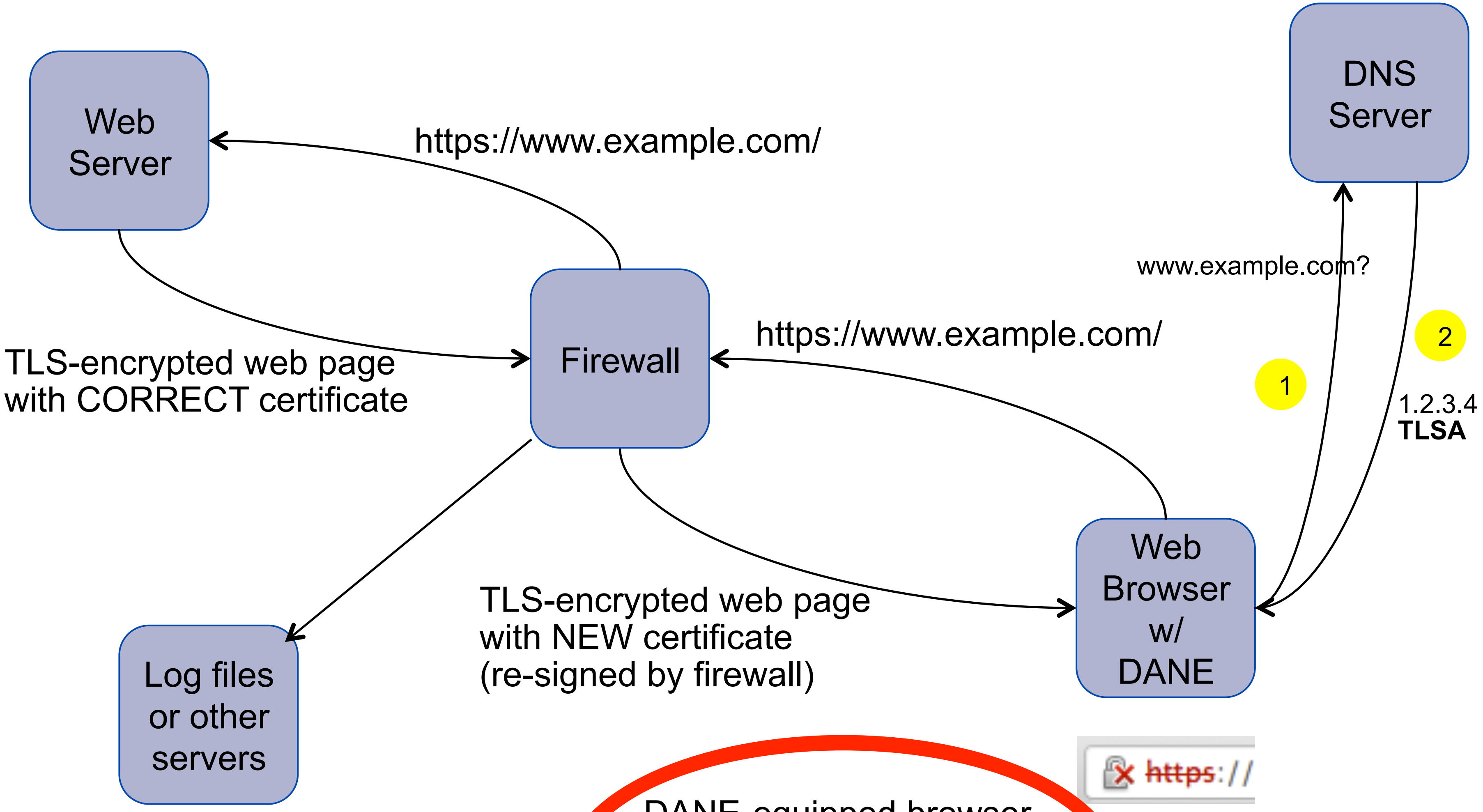
- Q: How do you know if the TLS (SSL) certificate is the correct one the site wants you to use?

- A: Store the certificate (or keys used) in DNS and sign them with DNSSEC.

A browser 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.

DANE


Web Server
https://www.example.com/
DNS Server
www.example.com?
TLS-encrypted web page with CORRECT certificate
Firewall
https://www.example.com/
1
2
1.2.3.4
TLSA
Web Browser w/ DANE
TLS-encrypted web page with NEW certificate (re-signed by firewall)
Log files or other servers
~~https~~://

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

DANE – Not Just For The Web

- DANE defines protocol for storing TLS certificates in DNS
- Securing Web transactions is the obvious use case
- Other uses also possible:
  - Email via S/MIME
  - VoIP
  - Jabber/XMPP
  - ?

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**

How Do We Get DANE Deployed?

Developers:

- Add DANE support into applications (see list of libraries)

DNS Hosting Providers:

- Provide a way that customers can enter a “TLSA” record into DNS as defined in RFC 6698 (http://tools.ietf.org/html/rfc6698)
- This will start getting TLS certificates into DNS so that when browsers support DANE they will be able to do so.
- [More tools are needed to help create TLSA records – ex. hashslinger]

Network Operators / Enterprises / Governments:

- Start talking about need for DANE
- Express desire for DANE to app vendors (especially browsers)

Next Steps

New Industry Initiative Forming With Focus On:

1. **Deployment Documentation**
   - What do we need in the way of better documentation/tutorials/etc ?
2. **Tools**
   - What are the missing tools?
3. **Unsolved Technical Issues**
   - What technical issues remain that need to be addressed?
4. **Measurement**
   - How do we measure progress of DNSSEC deployment?
   - Can we get more TLDs, ISPs to help provide statistics?

Join The Initial Discussions

Public mailing list, “dnssec-coord”, available and open to all:

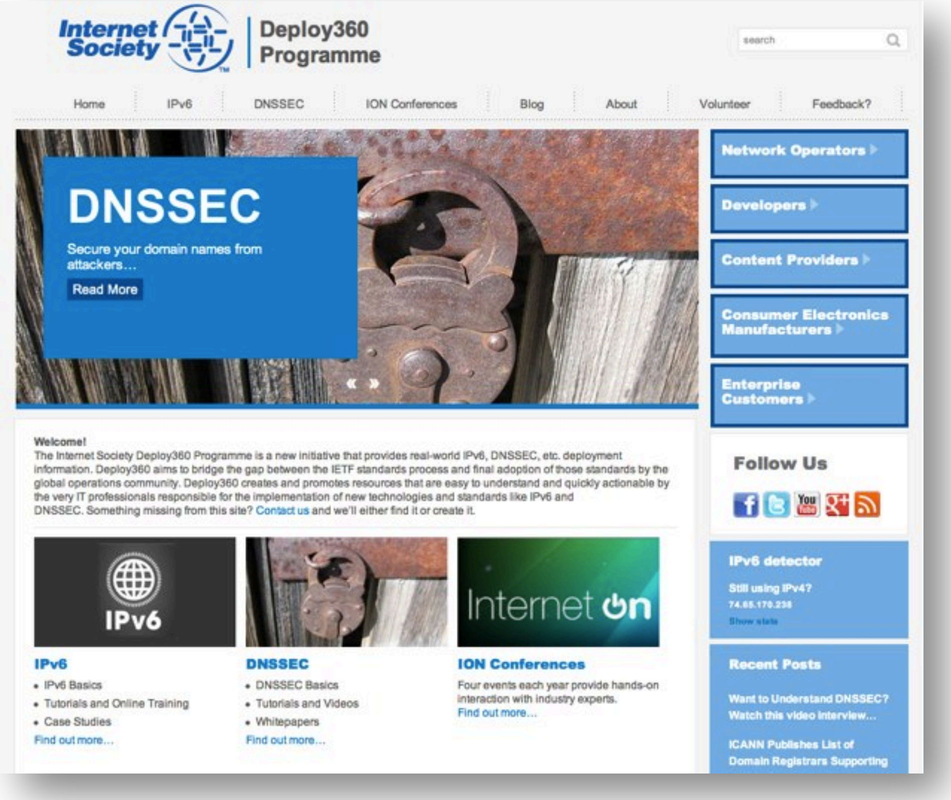
https://elists.isoc.org/mailman/listinfo/dnssec-coord

Focus is on better coordinating promotion / advocacy / marketing activities related to DNSSEC deployment.

Planning for monthly conference calls to support online activities.

Stay tuned for more info… (and join the list!)

Internet Society Deploy360 Programme



DNSSEC

Secure your domain names from attackers…

Welcome!
The Internet Society Deploy360 Programme is a new initiative that provides real-world IPv6, DNSSEC, etc. deployment information. Deploy360 aims to bridge the gap between the IETF standards process and final adoption of those standards by the global operations community. Deploy360 creates and promotes resources that are easy to understand and quickly actionable by the very IT professionals responsible for the implementation of new technologies and standards like IPv6 and DNSSEC. Something missing from this site? Contact us and we'll either find it or create it.

IPv6
- IPv6 Basics
- Tutorials and Online Training
- Case Studies

Find out more…

DNSSEC
- DNSSEC Basics
- Tutorials and Videos
- Whitepapers

Find out more…

ION Conferences
Four events each year provide hands-on interaction with industry experts.
Find out more…

Follow Us

IPv6 detector
Still using IPv4?
74.65.170.238
Show stats

Recent Posts
Want to Understand DNSSEC? Watch this video interview…
ICANN Publishes List of Domain Registrars Supporting

www.internetsociety.org/deploy360/

Can You Help Us With:

- Case Studies?
- Tutorials?
- Videos?

How Can We Help You?

Dan York, CISSP

Senior Content Strategist, Internet Society

york@isoc.org

www.internetsociety.org/deploy360/

Thank You!

Additional Material

Review Our DNSSEC Content Roadmap

We have posted a roadmap of the content we believe we need to add to Deploy360 site related to DNSSEC (and IPv6):

www.internetsociety.org/deploy360/roadmap/

We would greatly appreciate feedback:

- Anything missing? Are there additional topics we should consider?
- Will this content help you deploy DNSSEC?
- Please send comments to **deploy360@isoc.org**

Download A DNSSEC Whitepaper

"Challenges and Opportunities in Deploying DNSSEC"

http://bit.ly/isoc-satin2012

Other Areas (Beyond Those Mentioned Earlier)

- Tools exist to help automate key signing (ex. OpenDNSSEC)
- The “key rollover” process needs to be well-documented (ex. NASA/Comcast issue)
- Guidance can be found in “DNSSEC Policy & Practice Statements” (often abbreviated “DPS”)
    - http://www.internetsociety.org/deploy360/resources/dnssec-practice-statements/