Keys, Hollywood and History: The truth about ICANN, DNSSEC, and the Root Key

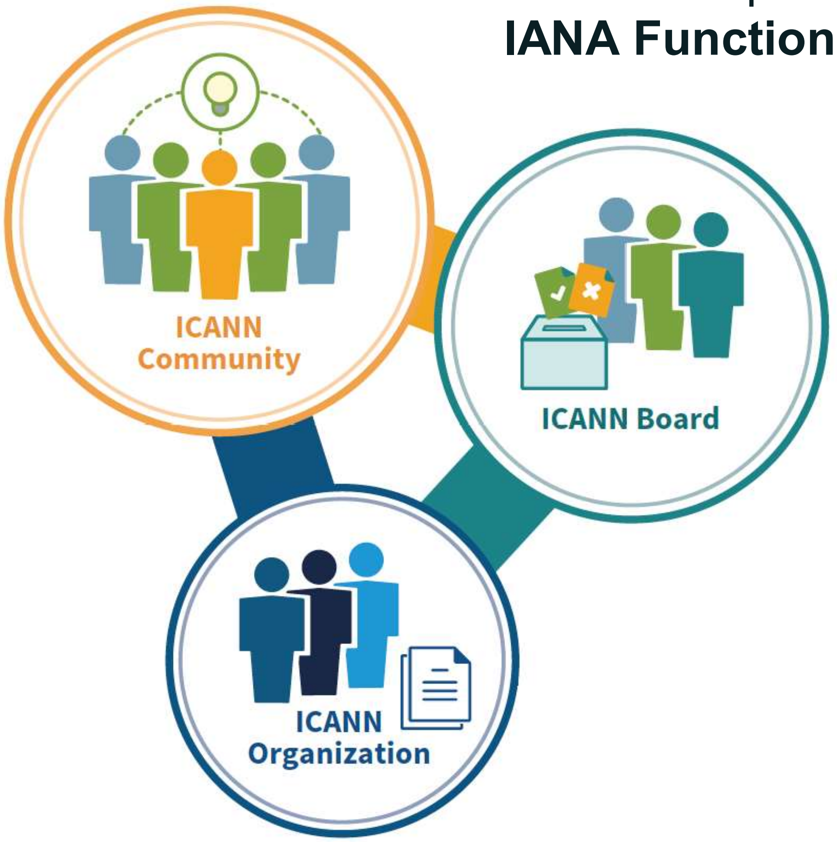
Dr. Richard Lamb

Sonoma State University
November 2017

What Hollywood Sees – part 1

What is ICANN?

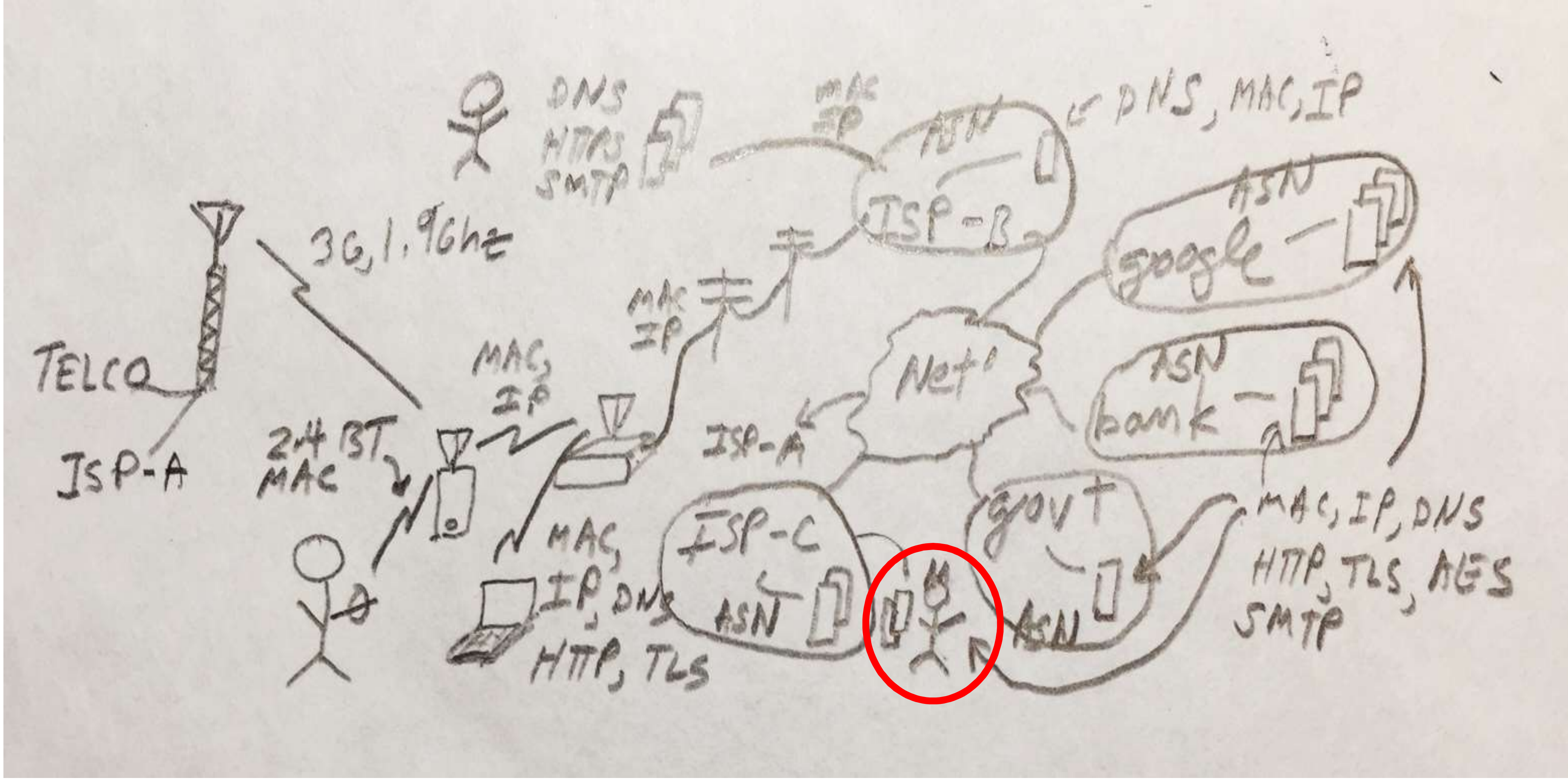
Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the top-level of the Internet's system of unique identifiers via global, multistakeholder, bottom-up consensus policy process, which is implemented via the **IANA Functions**



Internet Assigned Numbers Authority (**IANA**) **Functions**

- Protocol Parameters
- Number Resources
- Domain Name

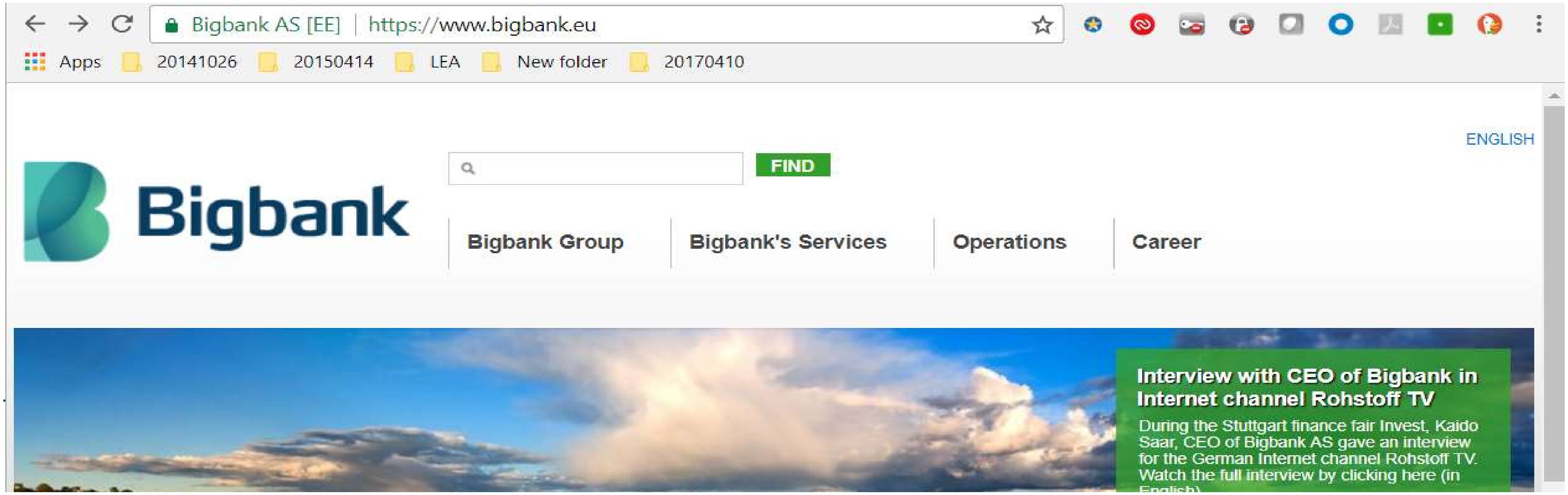
We all start with a cocktail napkin



Media was focused on looking up names to numbers

The Domain Name System: DNS

- DNS converts names (www.bigbank.eu) to numbers (213.168.0.51)
- ..to identify services such as www and e-mail
- ..that identify and link customers to business and visa versa



Interview with CEO of Bigbank in Internet channel Rohstoff TV

During the Stuttgart finance fair Invest, Kaido Saar, CEO of Bigbank AS gave an interview for the German Internet channel Rohstoff TV. Watch the full interview by clicking here (in English)

DNS is a part of all IT ecosystems (much more than one expects)

IoT

US-NSTIC effort

Google

OpenID

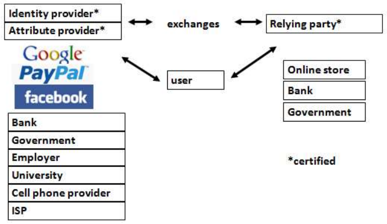
facebook

HealthCare.gov

ebay

AADHAAR

OECS ID effort



Identity provider*
Attribute provider*
exchanges
Relying party*
Google
PayPal
facebook
user
Bank
Government
Employer
University
Cell phone provider
ISP
Online store
Bank
Government
*certified

PayPal

amazon Prime

e-Passport symbol

ICP Brasil

O Brasil na era da certificação digital

DigiNotar

A VASCO COMPANY

COMODO

Creating Trust Online

Norton SECURED

powered by VeriSign

O chip perm
armazenam
dados sobre

DATA NASCIMENTO
10/06/1975
FILIAÇÃO
JOÃO CARVALHO
MARIA CARVALHO

SVERIGE SWEDEN SUÈDE
Nationellt identitetskort/National identity card/Carte nationale d'identité
Nationalitet/Nationality
SVENSK/SWE
Kortnummer/Card No.
45123456
Personnr./Personal Id. No.
610321-3499
Innehavarens namnteckning/Holder's signature
Längd/Height
177 CM
Födelsedatum/Date of birth
21 MAR/MAR 61
Kön/Sex
M/M
Efternamn/Surname
SPECIMEN
Förnamn/Given names
SVEN
Myndighet/Authority
POLISMYNDIGHETEN I STOCKHOLMS LÄN
Utfärdat/Date of issue
25 JUL/JUL 07
Giltigt t.o.m./Date of expiry
25 JUL/JUL 12
SPECIMEN

För kontrol
For check c
Swedish Po
IF FOUND,
Rikspolisstyr

Trust frameworks are not new

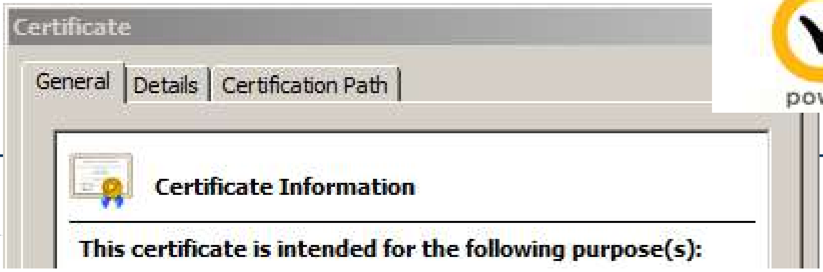
Identity providers
Exchange (clearing house)
Relying parties
TOK&STOK
C&C casa&construção
amazon.com
macys

EESTI VABARIIK
REPUBLIC OF ESTONIA
ISIKUTUNNISTUS
IDENTITY CARD
PEREKONNANIMI/SURNAME
MÄNNIK
EESNIMED/GIVEN NAMES
MARI-LIIS
SUGU/SEX
N/F
KODAKONDSUS/CITIZENSHIP
EST
SÜNNIAEG/DATE OF BIRTH
01.01.1971
ISIKUKOOD/PERSONAL CODE
47101010033
DOKUMENDI NUMBER/DOCUMENT NUMBER
A1410634
KEHTIV KUNI/DATE OF EXPIRY
21.02.2012
KASUTAJA ALLKIRI/HOLDER'S SIGNATURE
SPECIMEN

ARVALHO<FERNANDA<<<<<<

mydomainname.co

Smart Electrical Grid



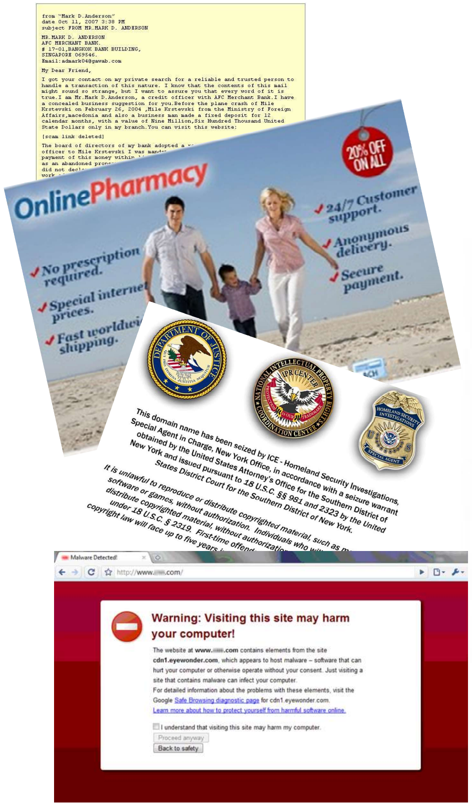
Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

..and used for all sorts of purposes
Not all good



from "Mark D.Anderson"
date Oct 11, 2007 3:38 PM
subject FROM MR.MARK D. ANDERSON

MR.MARK D. ANDERSON
AFC MERCHANT BANK.
17-01,BANGKOK BANK BUILDING,
SINGAPORE 069546.
Email:admark04@gawab.com

My Dear Friend,

I got your contact on my private search for a reliable and trusted person to handle a transaction of this nature. I know that the contents of this mail might sound so strange, but I want to assure you that every word of it is true.I am Mr.Mark D.Anderson, a credit officer with AFC Merchant Bank.I have a concealed business suggestion for you.Before the plane crash of Mile Krstevski on February 26, 2004 ,Mile Krstevski from the Ministry of Foreign Affairs,macedonia and also a business man made a fixed deposit for 12 calendar months, with a value of Nine Million,Six Hundred Thousand United State Dollars only in my branch.You can visit this website:

[scam link deleted]

The board of directors of my bank adopted a
officer to Mile Krstevski I was mand
payment of this money within
as an abandoned prope
did not decl
work

This domain name has been seized by ICE - Homeland Security Investigations, Special Agent in Charge, New York Office, in accordance with a seizure warrant obtained by the United States Attorney's Office for the Southern District of New York and issued pursuant to 18 U.S.C. §§ 981 and 2323 by the United States District Court for the Southern District of New York.

It is unlawful to reproduce or distribute copyrighted material, such as m software or games, without authorization. Individuals who wi distribute copyrighted material, without authorization under 18 U.S.C. § 2319. First-time offend copyright law will face up to five years

Warning: Visiting this site may harm your computer!

The website at **www.[redacted].com** contains elements from the site **cdn1.eyewonder.com**, which appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that contains malware can infect your computer.

For detailed information about the problems with these elements, visit the Google Safe Browsing diagnostic page for cdn1.eyewonder.com.

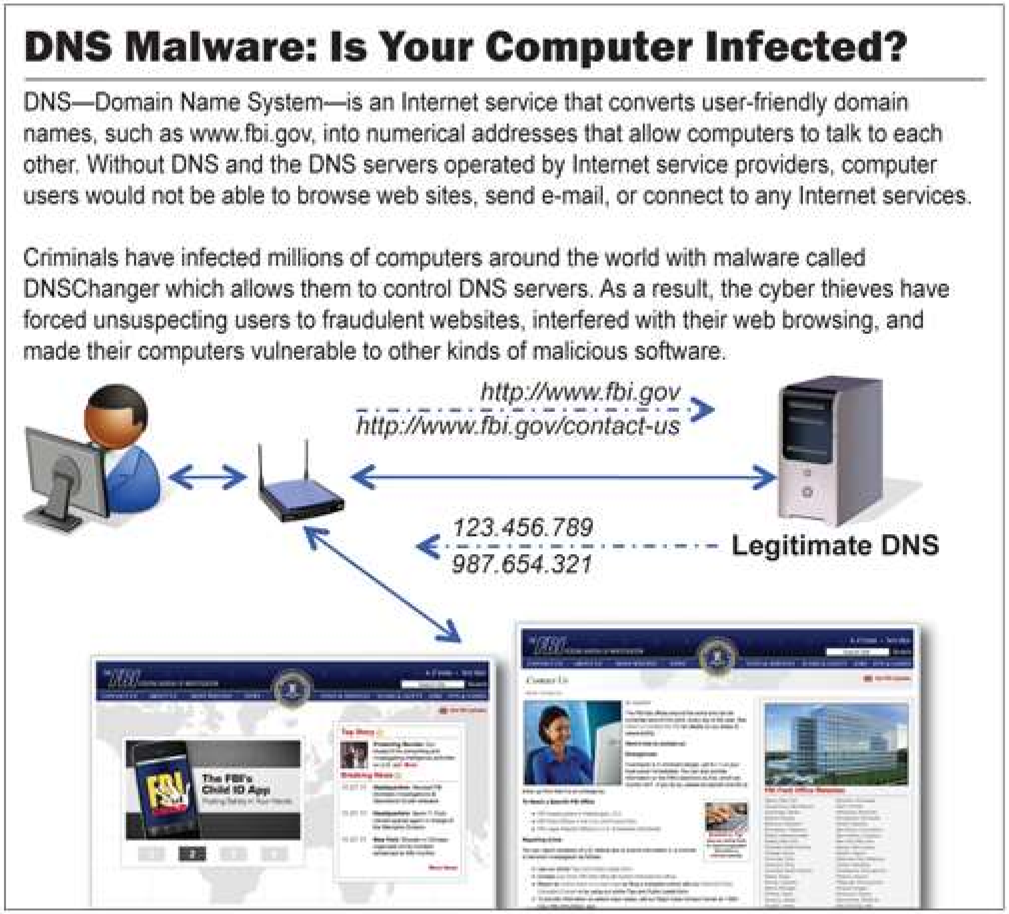
Learn more about how to protect yourself from harmful software online.

□ I understand that visiting this site may harm my computer.

Domains registered by criminals for

- Counterfeit goods
- Data exfiltration
- Exploit attacks
- Illegal pharma
- Infrastructure (ecrime name resolution)
- Malware C&C
- Malware distribution, ransomware
- Phishing, Business Email Compromise
- Scams (419, reshipping, stranded traveler…)

E.g, DNSChanger - ‘Biggest Cybercriminal Takedown in History’ – 4M machines, 100 countries



DNS Malware: Is Your Computer Infected?

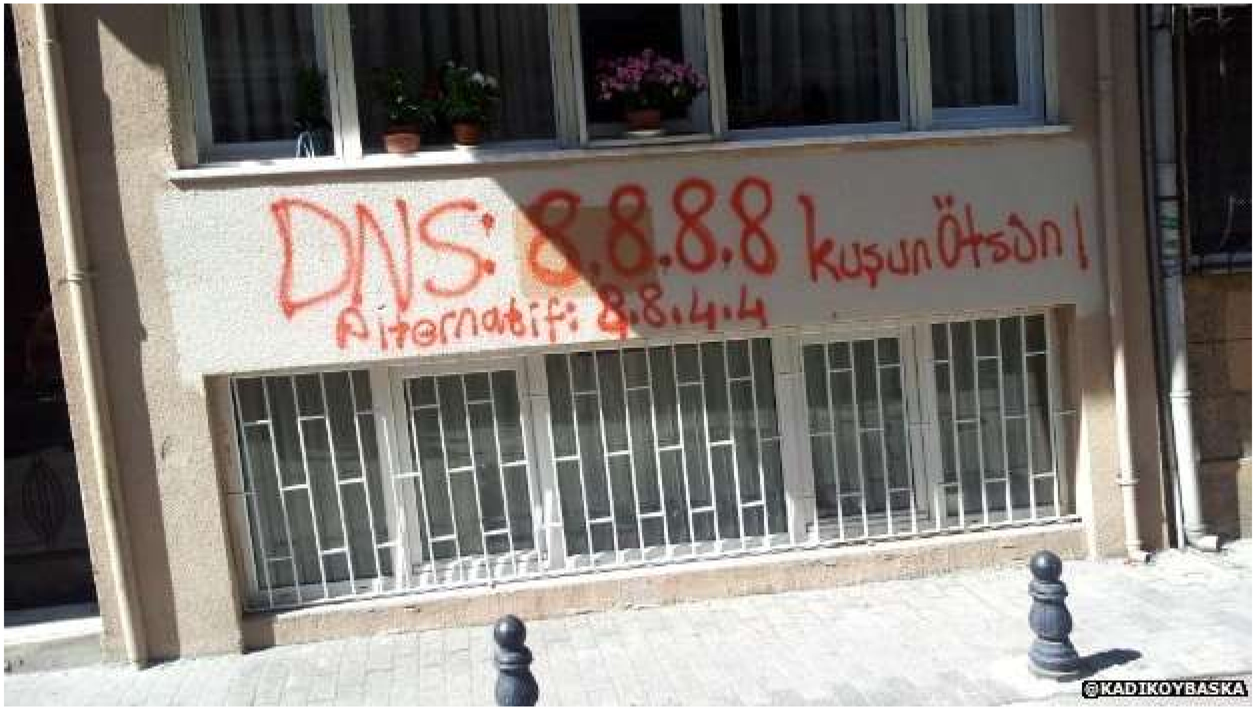
DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

Nov 2011 http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/

End-2-end DNSSEC validation would have avoided the problems

Man-in-the-middle attacks on DNS



That darn press ;-)

Other DNS hijacks*

- 25 Dec 2010 - Russian e-Payment Giant ChronoPay Hacked
- 18 Dec 2009 – Twitter – “Iranian cyber army”
- 13 Aug 2010 - Chinese gmail phishing attack
- 25 Dec 2010 Tunisia DNS Hijack
- 2009-2012 google.*
  - April 28 2009 Google Puerto Rico sites redirected in DNS attack
  - May 9 2009 Morocco temporarily seize Google domain name
- 9 Sep 2011 - Diginotar certificate compromise for Iranian users
- SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate. Unfortunately, majority of Web site certificates rely on DNS to validate identity.
- DNS is relied on for unexpected things though insecure.

*A Brief History of DNS Hijacking - Google
http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf

Oops - 2008@DEFCON (Dan Kaminsky + Press)

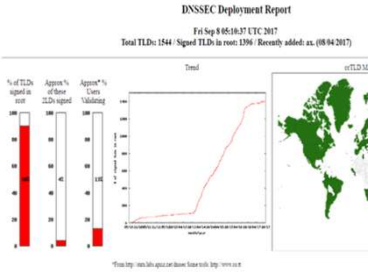
- Dan exploits flaw in the DNS @DEFCON
- CPU and bandwidth advances made legacy DNS vulnerable to MITM attacks
- Lots of press! Barriers to deployment of DNSSEC seem to disappear.

https://en.wikipedia.org/wiki/Dan_Kaminsky
https://blog.cloudflare.com/dnssec-an-introduction/

Secure the DNS?

DNS Security Extensions - DNSSEC

- A humble bottom-up effort by techies that is now on 90% of the Internet’s core infrastructure.
- Encouraged by many governments
- Required by ICANN



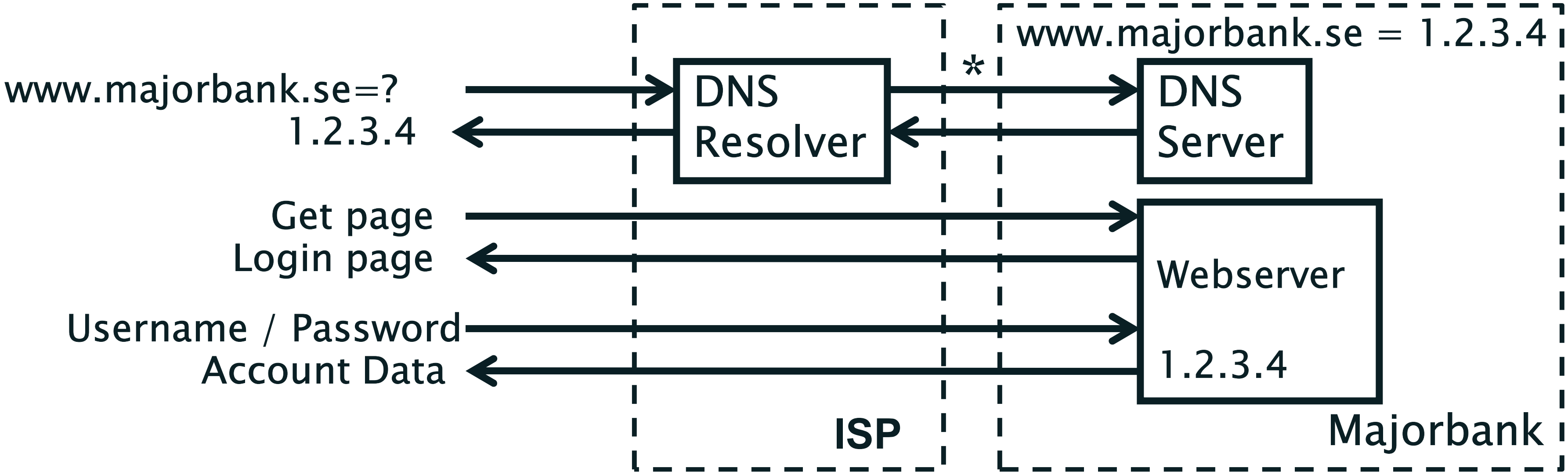
DNSSEC Deployment Report

Fri Sep 8 05:10:37 UTC 2017
Total TLDs: 1544 / Signed TLDs in root: 1396 / Recently added: ax. (08/04/2017)

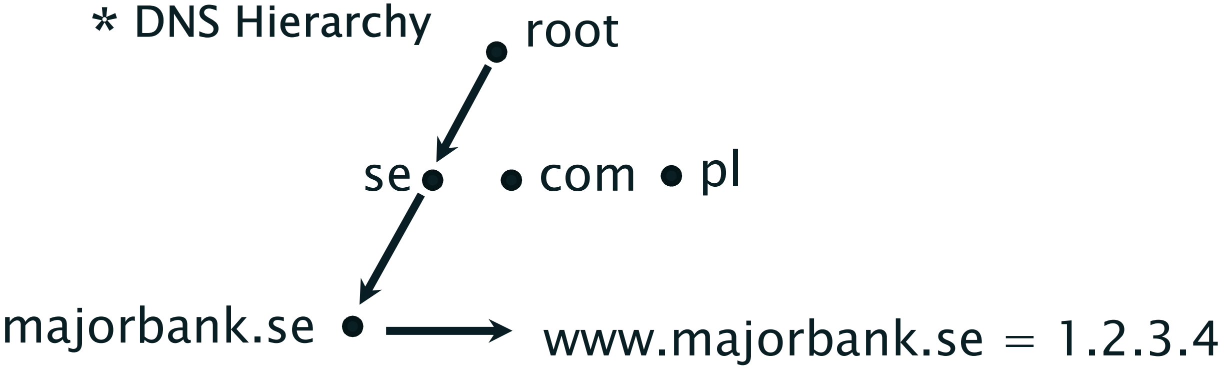
*From http://stats.labs.apnic.net/dnssec Some tools: http://www.cz.tt

To make sure everyone gets what they asked for from the Internet’s phonebook

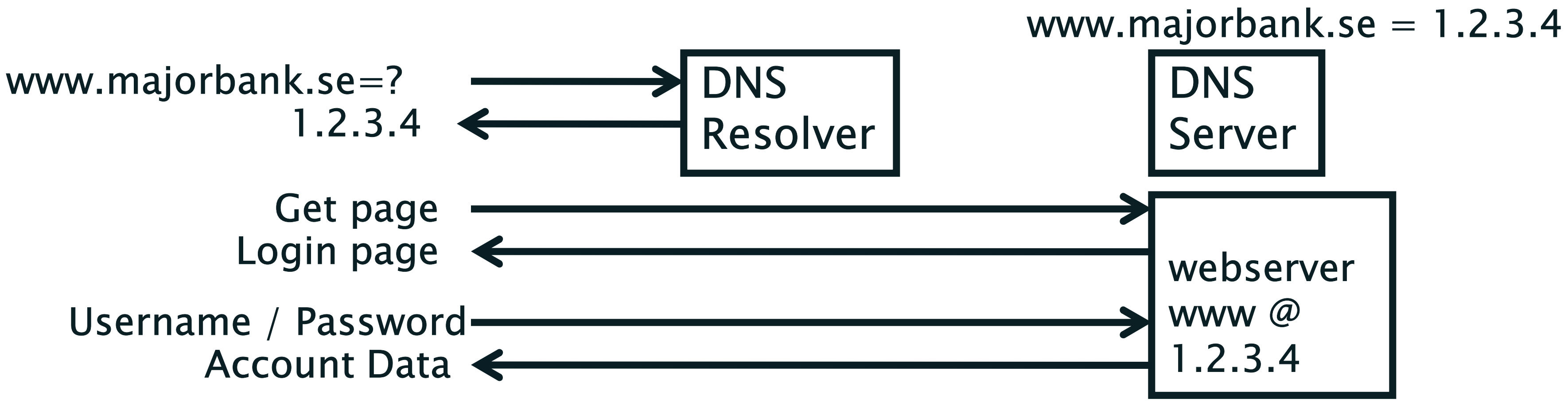
The Internet’s Phone Book - Domain Name System (DNS)



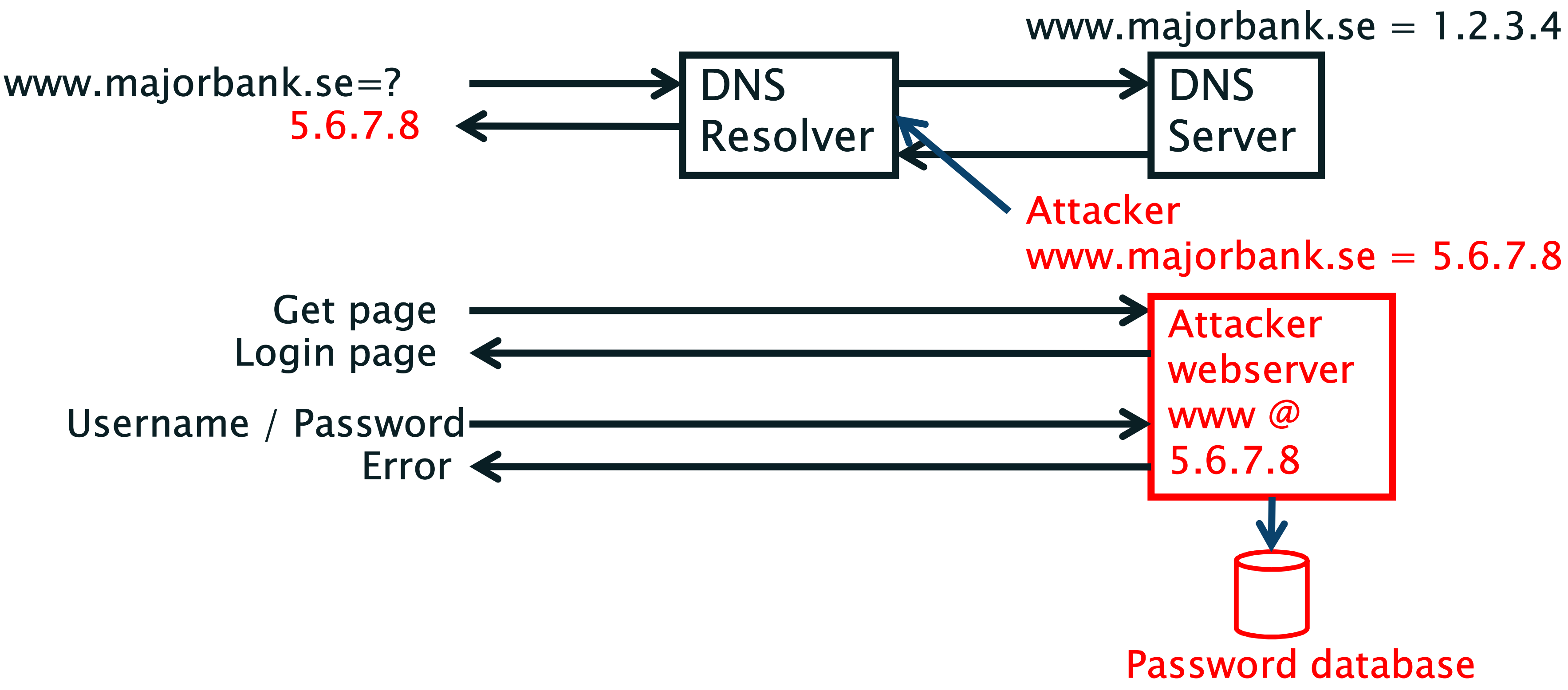
* DNS Hierarchy



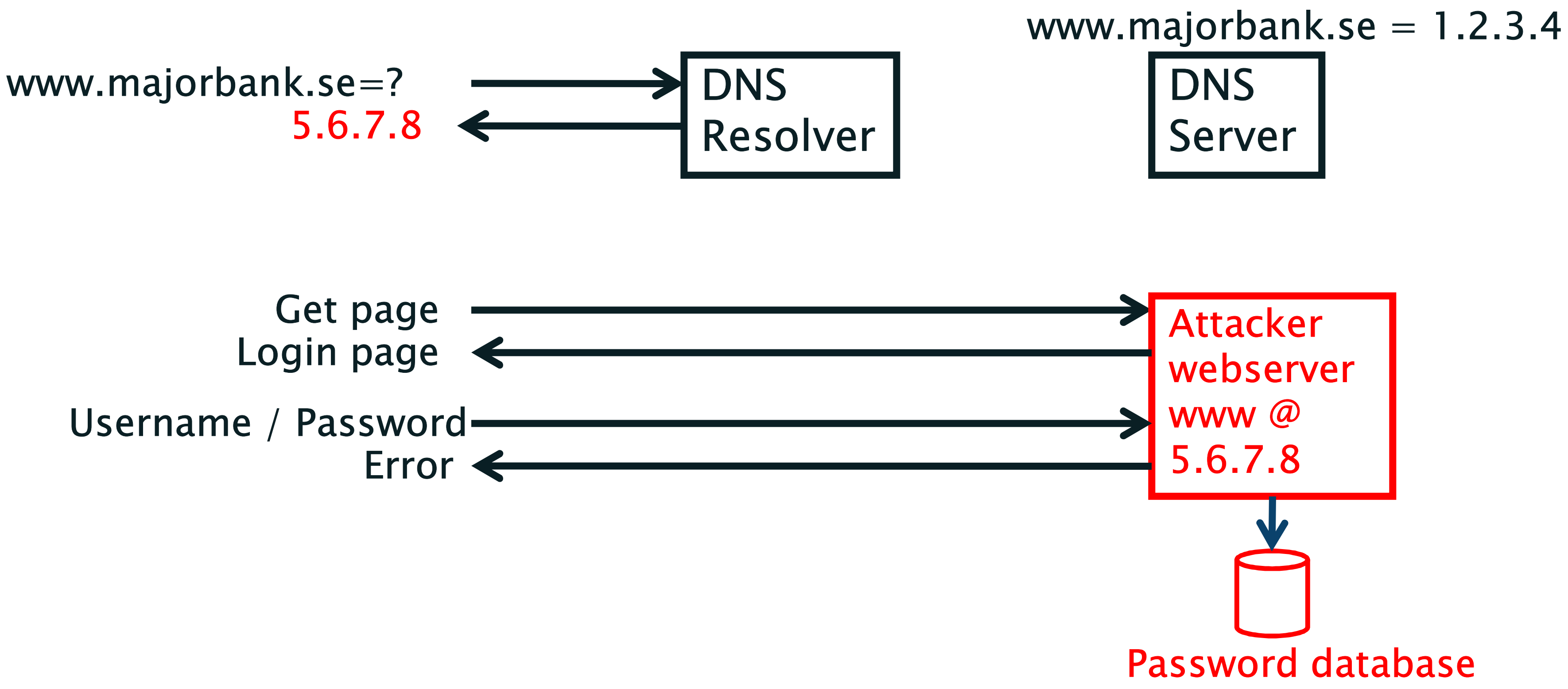
Caching Responses for Efficiency



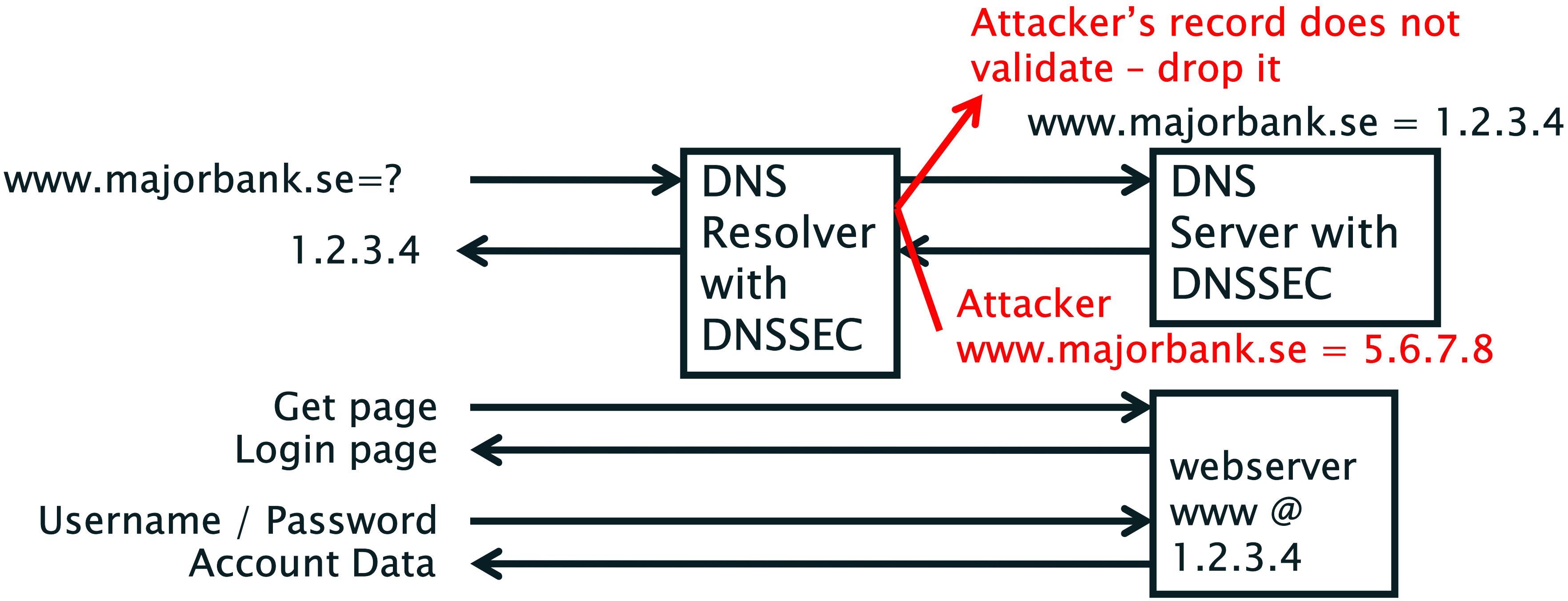
The Problem: DNS Cache Poisoning Attack



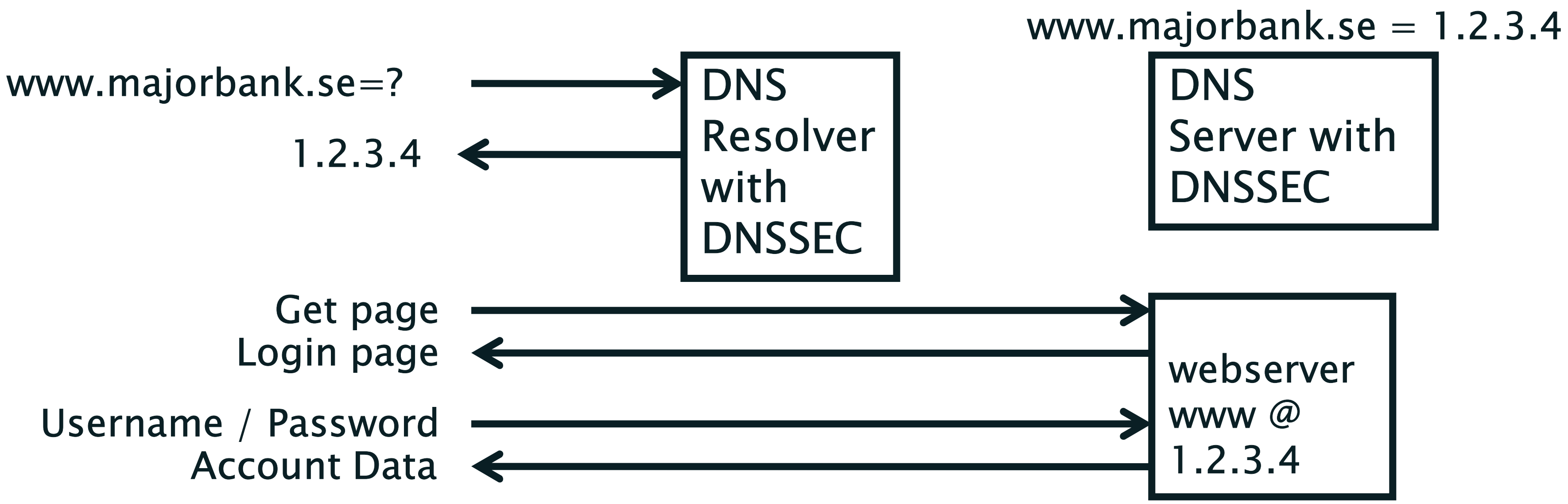
Argghh! Now all ISP customers get sent to attacker.



Securing The Phone Book
DNS Security Extensions (DNSSEC)



Resolver only caches validated records



www.majorbank.se=?

1.2.3.4

DNS Resolver with DNSSEC

www.majorbank.se = 1.2.3.4

DNS Server with DNSSEC

Get page

Login page

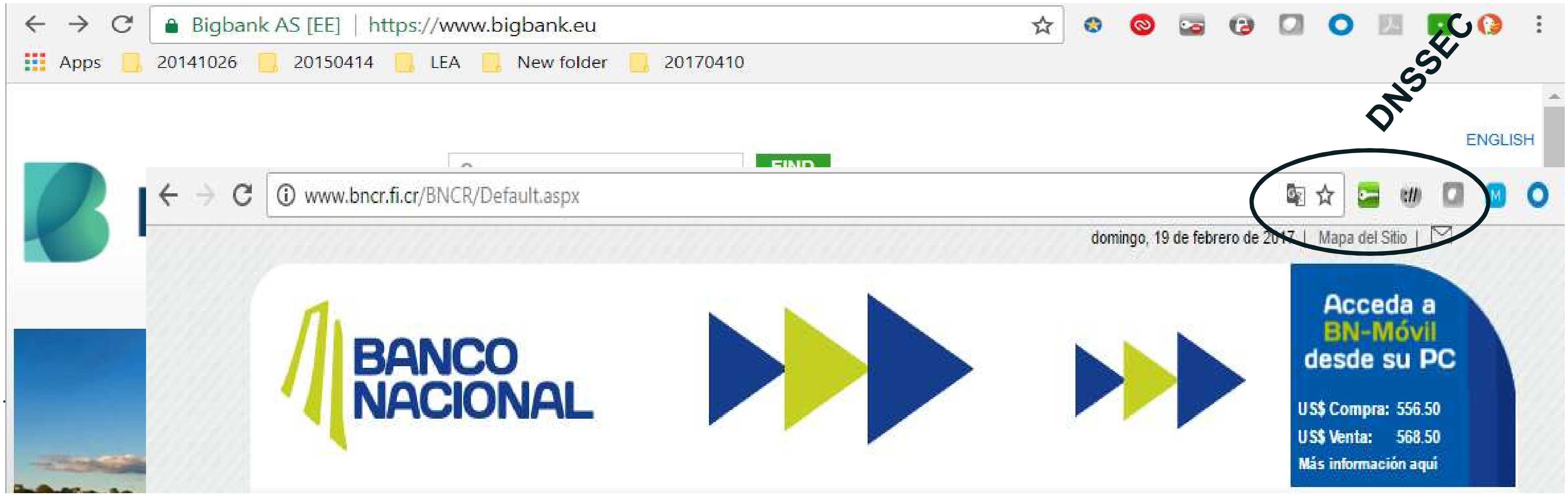
Username / Password

Account Data

webserver www @ 1.2.3.4

Securing it

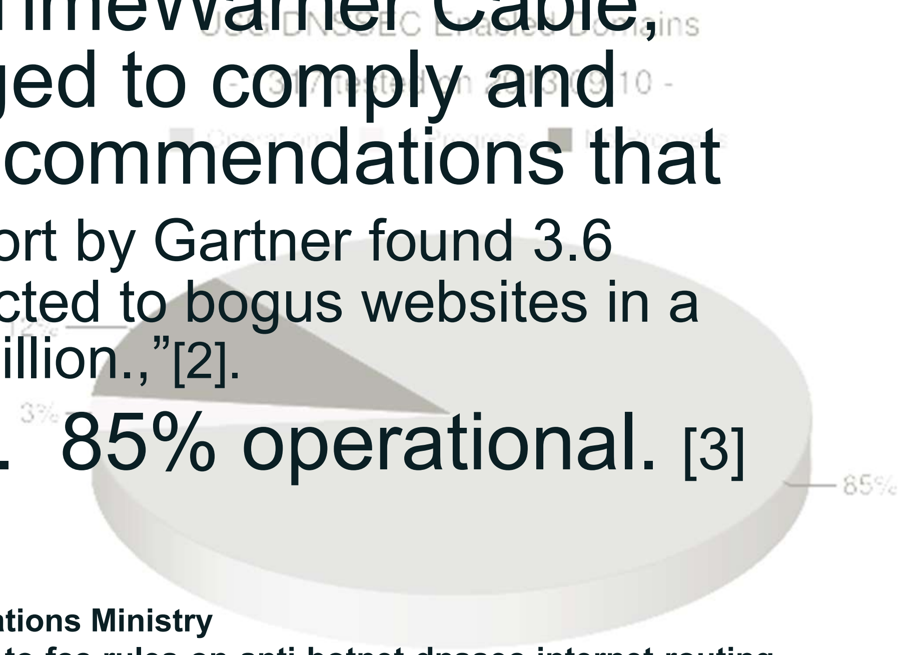
- DNS converts names (www.bncr.fi.cr) to numbers (201.220.29.26)
- Make sure we get the right numbers (DNSSEC)
- Verify the identity and encrypt data



Bigbank AS [EE] | https://www.bigbank.eu
Apps
20141026
20150414
LEA
New folder
20170410
ENGLISH
FIND
www.bncr.fi.cr/BNCR/Default.aspx
DNSSEC
domingo, 19 de febrero de 2017 | Mapa del Sitio |
BANCO NACIONAL
Acceda a BN-Móvil desde su PC
US$ Compra: 556.50
US$ Venta: 568.50
Más información aquí

DNSSEC interest from governments

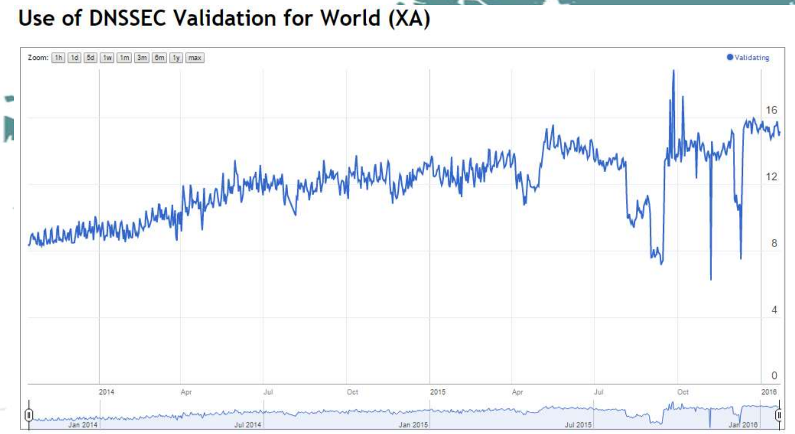
- Sweden, Brazil, Netherlands, Czech Republic and others encourage DNSSEC deployment to varying degrees
- Mar 2012 - AT&T, CenturyLink (Qwest), Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC [1] recommendations that include DNSSEC.. “A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.,”[2].
- 2008 US .gov mandate. 85% operational. [3]



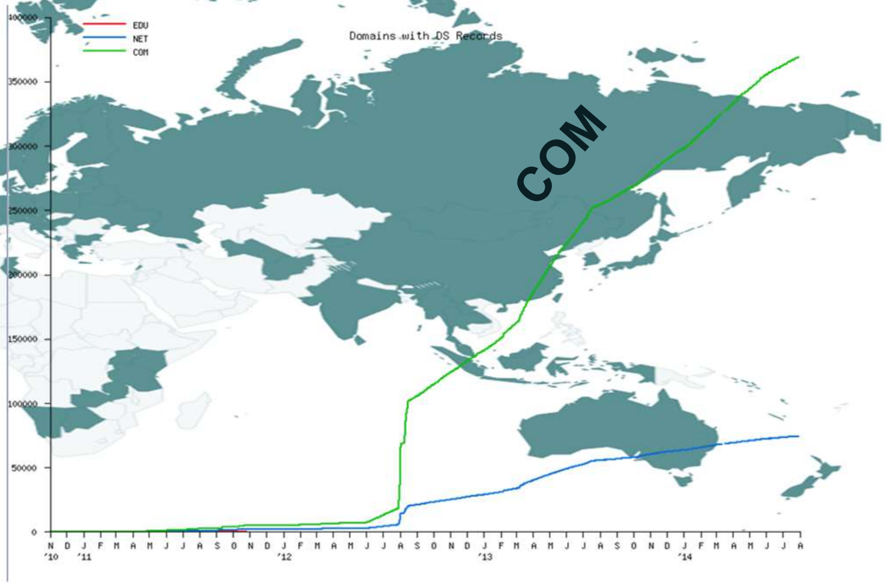
[1] FCC=Federal Communications Commission=US communications Ministry

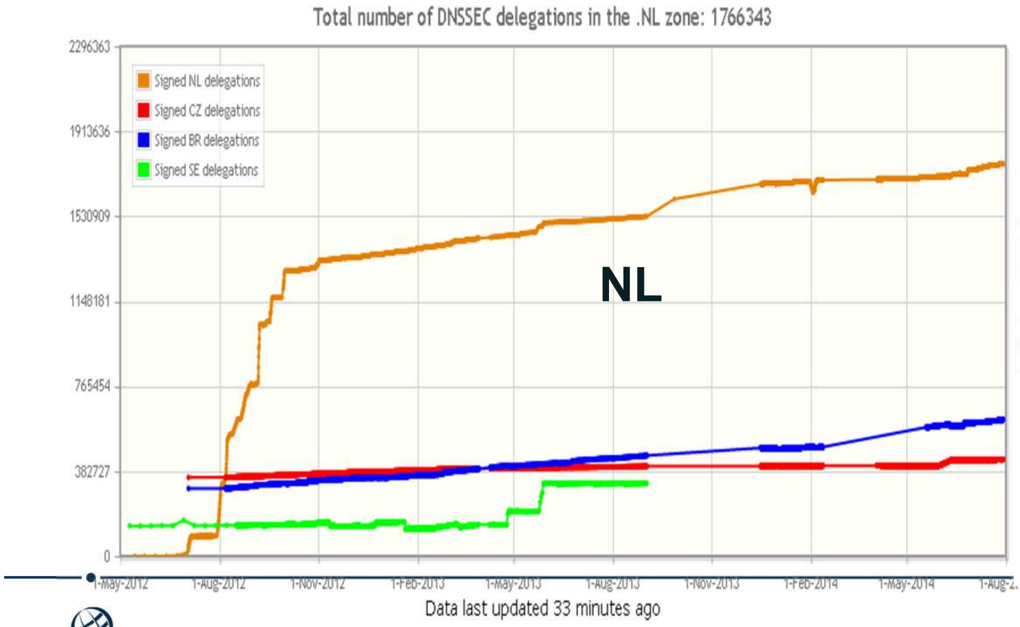
[2] http://securitywatch.pcmag.com/security/295722-isps-agree-to-fcc-rules-on-anti-botnet-dnssec-internet-routing

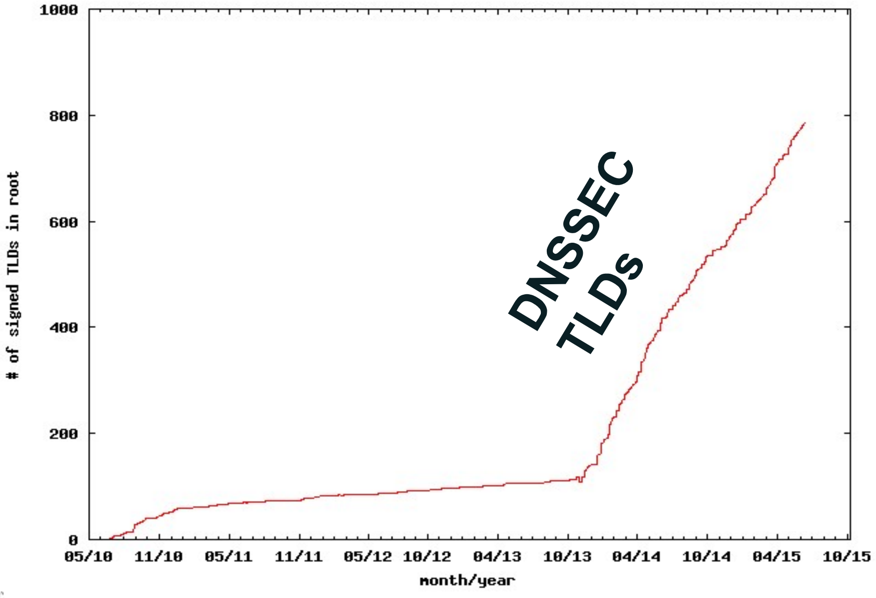
[3] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf
http://fedv6-deployment.antd.nist.gov/snap-all.html

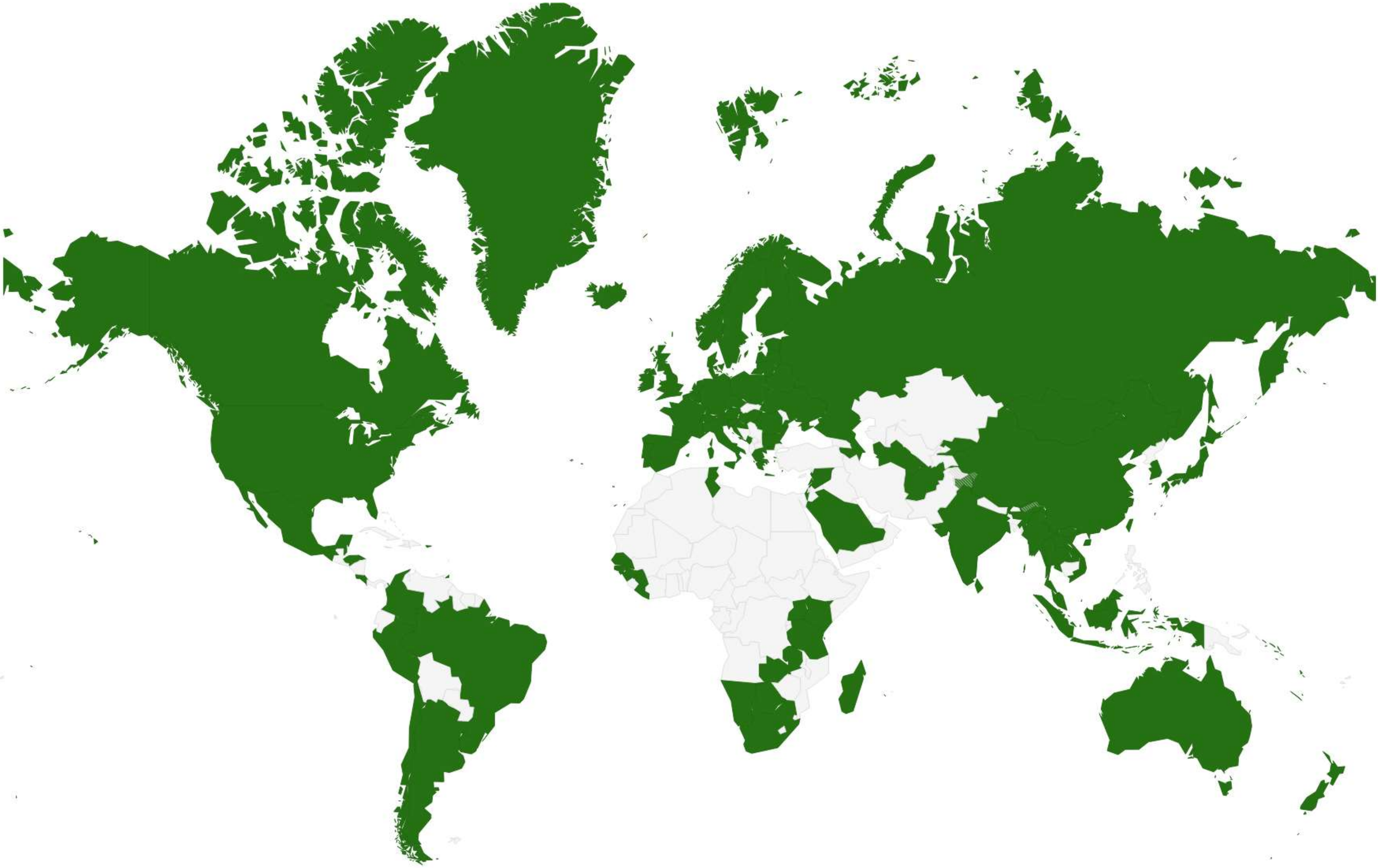


Thank you Geoff Huston









DNSSEC - Where we are

- Deployed on 1395/1541 TLDs (8 Nov 2017 .it .ax .sa .vn .cn .jp .nz .la .mm .th .in .id .tw .au .sg .lk .se .de .ru .рф .com .uk .nl .fr .us .my مليسيا .asia .tw 台灣, .kr 한국 .net, .org, .post, +ntlds, .ibm .berlin)
- Root signed** and audited
- 90% of domain names could have DNSSEC
- Required in new gTLDs. Basic support by ICANN registrars
- Growing ISP support* - ~15% end users "validate".
- 3rd party signing solutions***
- Growing S/W H/W support: BIND, NSD, KNOT, Microsoft DNS, PowerDNS, InfoBlox, Nominum, Secure64…openssl, postfix, XMPP, mozilla: DANE support
- IETF standard on DNSSEC TLS certificates (RFC6698, RFC8162) and others
- Growing support from major players…(Apple iPhone/iPad, Google 8.8.8.8, hosting co Cloudflare DNSSEC by default, German email providers…)

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

* COMCAST /w 20M and others; most ISPs in SE ,CZ.

**Int'l bottom-up trust model /w 21 TCRs from: TT, BF, RU, CN, US, SE, NL, UG, BR, Benin, PT, NP, Mauritius, CZ, CA, JP, UK, NZ…

But…

- But deployed on only ~3% of 2nd level domains. Many have plans. Few have taken the step (e.g., yandex.com, paypal.com*, comcast.com).
- DNSChanger and other attacks highlight today's need. (e.g end-2-end DNSSEC validation would have avoided the problems)
- Innovative security solutions (e.g., DANE) highlight tomorrow's value.

Industry DNSSEC Enabled Domains
- 1069 tested on 2012.07.28 -
1%
0%

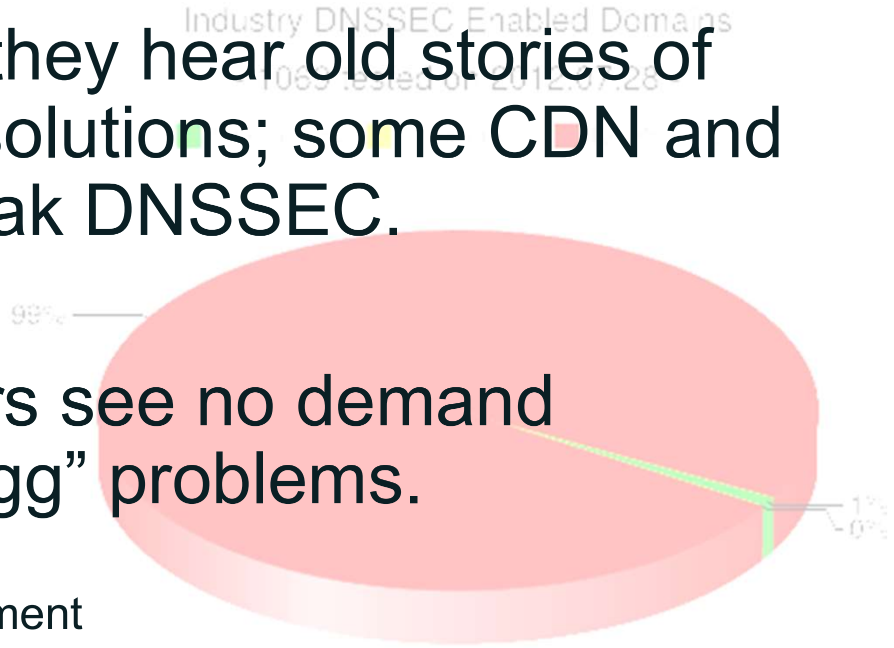
* http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-com
http://www.thesecuritypractice.com/the_security_practice/2011/12/all-paypal-domains-are-now-using-dnssec.html
http://www.nacion.com/2012-03-15/Tecnologia/Sitios-web-de-bancos-ticos-podran-ser-mas-seguros.aspx

DNSSEC: So what’s the problem?

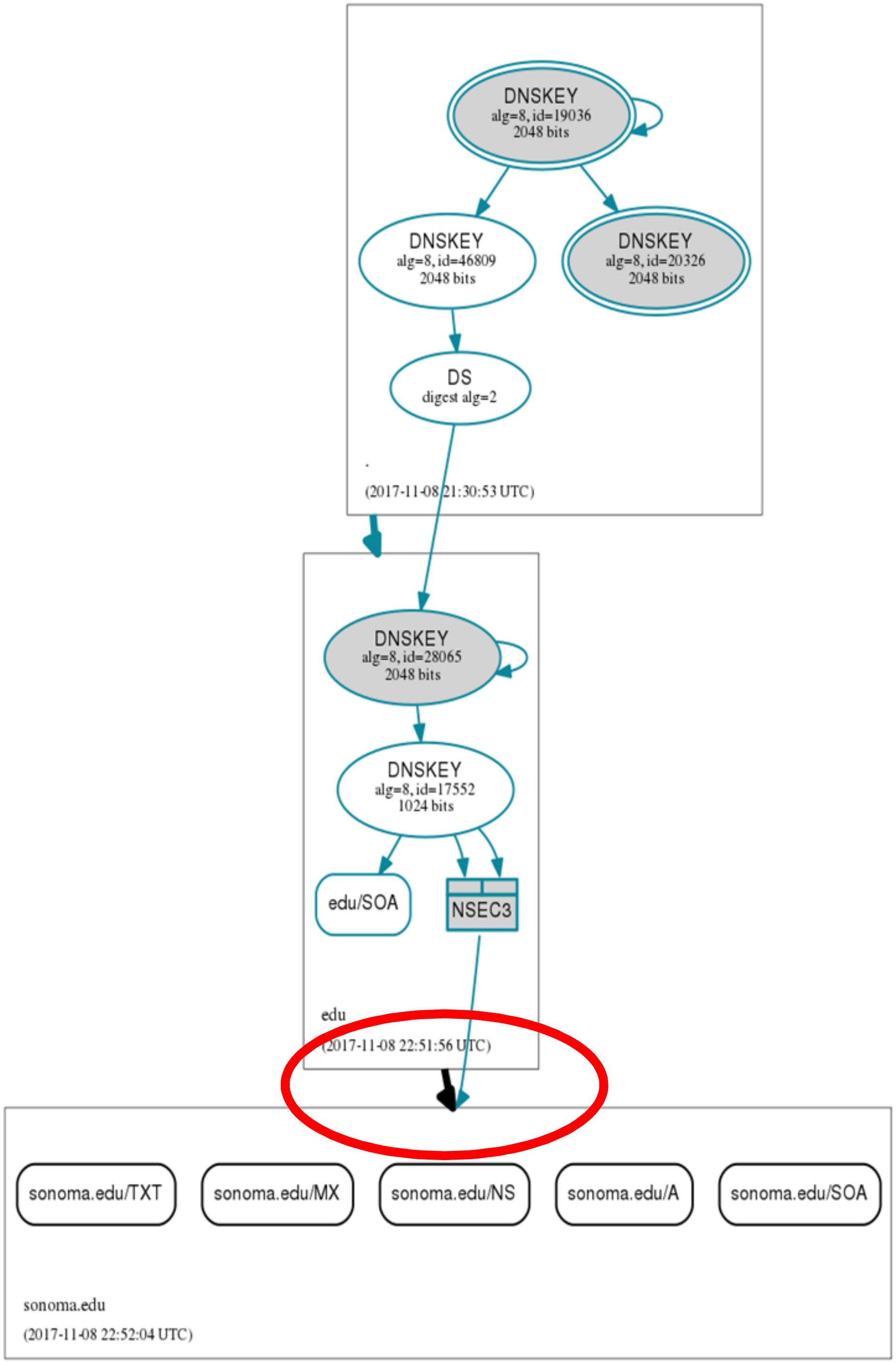
- Not enough IT departments know about it or are too busy putting out other security fires.

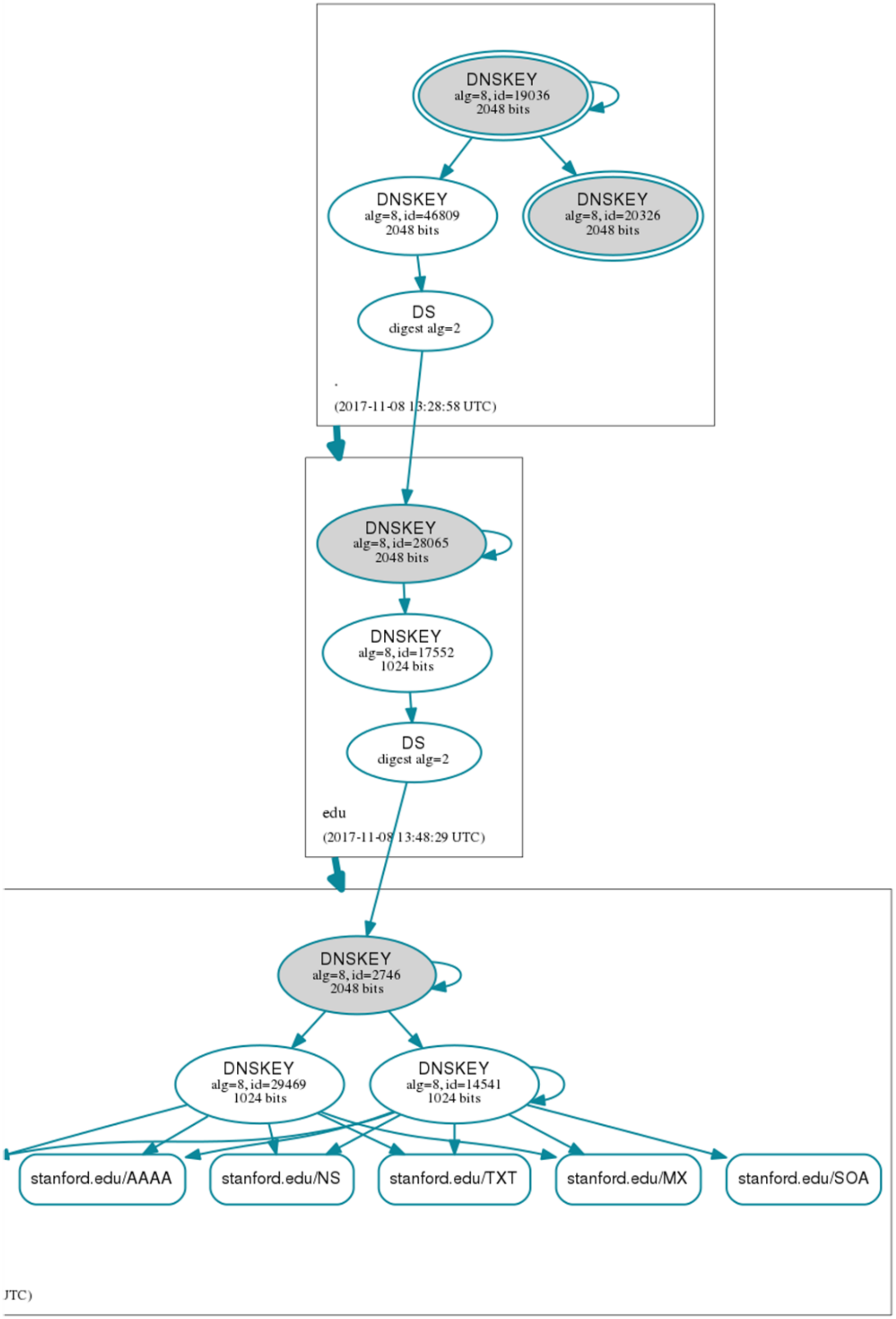
- When they do look into it they hear old stories of FUD and lack of turnkey solutions; some CDN and resolver architectures break DNSSEC.

- Registrars*/DNS providers see no demand leading to “chicken-and-egg” problems.



*but required by new ICANN registrar agreement


DNSKEY
alg=8, id=19036
2048 bits
DNSKEY
alg=8, id=46809
2048 bits
DNSKEY
alg=8, id=20326
2048 bits
DS
digest alg=2
.
(2017-11-08 21:30:53 UTC)
DNSKEY
alg=8, id=28065
2048 bits
DNSKEY
alg=8, id=17552
1024 bits
edu/SOA
NSEC3
edu
(2017-11-08 22:51:56 UTC)
sonoma.edu/TXT
sonoma.edu/MX
sonoma.edu/NS
sonoma.edu/A
sonoma.edu/SOA
sonoma.edu
(2017-11-08 22:52:04 UTC)


DNSKEY
alg=8, id=19036
2048 bits
DNSKEY
alg=8, id=46809
2048 bits
DNSKEY
alg=8, id=20326
2048 bits
DS
digest alg=2
.
(2017-11-08 13:28:58 UTC)
DNSKEY
alg=8, id=28065
2048 bits
DNSKEY
alg=8, id=17552
1024 bits
DS
digest alg=2
edu
(2017-11-08 13:48:29 UTC)
DNSKEY
alg=8, id=2746
2048 bits
DNSKEY
alg=8, id=29469
1024 bits
DNSKEY
alg=8, id=14541
1024 bits
stanford.edu/AAAA
stanford.edu/NS
stanford.edu/TXT
stanford.edu/MX
stanford.edu/SOA
JTC)

What you can do

- ***For Companies:***
  - – Sign your corporate domain names
  - – Just turn on validation on corporate DNS resolvers
- ***For Users:***
  - – Ask ISP to turn on validation on their DNS resolvers
- ***For All:***
  - – Take advantage of ICANN, ISOC and other organizations offering DNSSEC education and training

DNSSEC: A Global Platform for Innovation

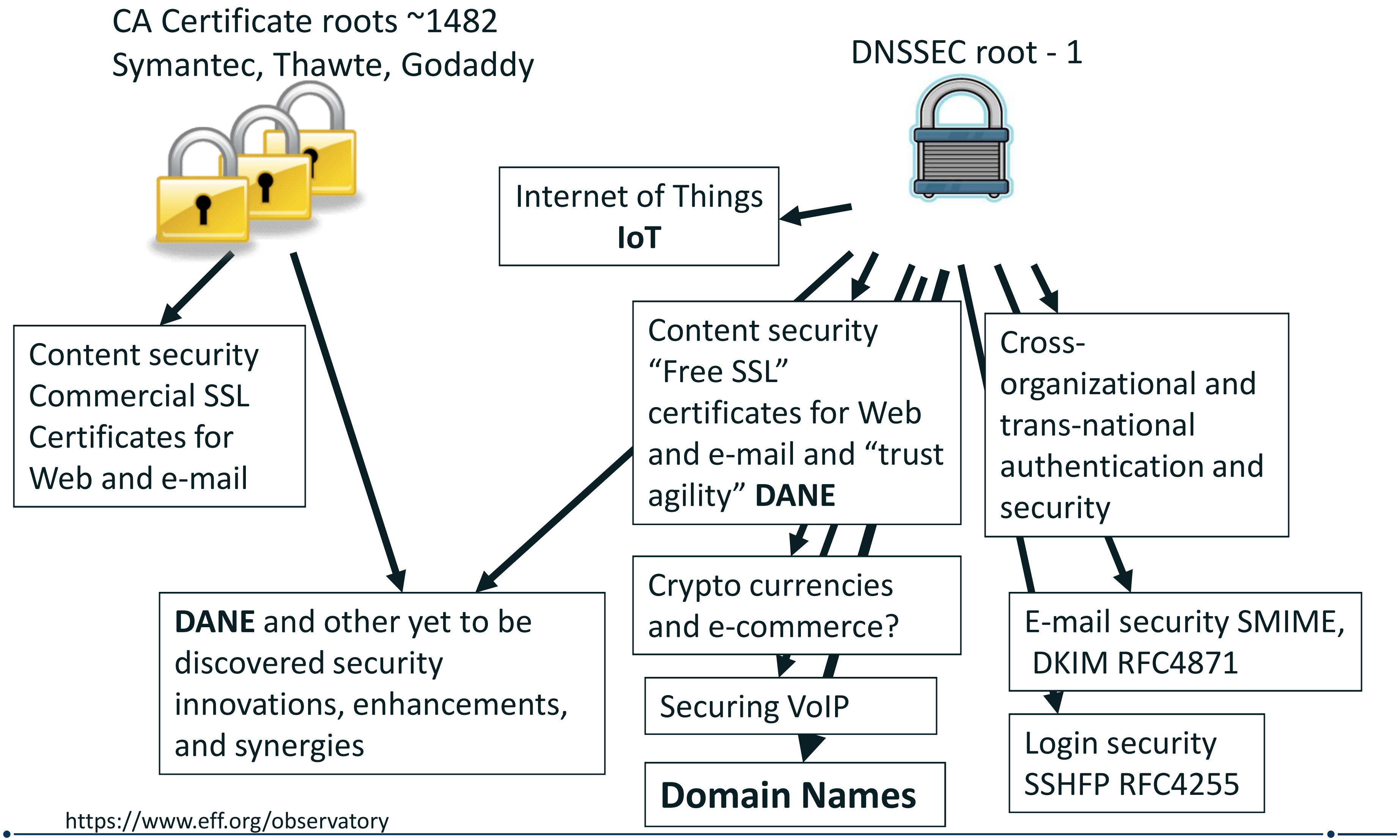
or..

I* $mell opportunity !

Game changing Internet Core Infrastructure Upgrade

- “More has happened here today than meets the eye. An infrastructure has been created for a hierarchical security system, which can be purposed and re-purposed in a number of different ways. ..” – Vint Cerf (June 2010)

Another source of trust on the Internet



CA Certificate roots ~1482
Symantec, Thawte, Godaddy

DNSSEC root - 1

Internet of Things
IoT

Content security
Commercial SSL
Certificates for
Web and e-mail

Content security
“Free SSL”
certificates for Web
and e-mail and “trust
agility” **DANE**

Cross-organizational and trans-national authentication and security

DANE and other yet to be discovered security innovations, enhancements, and synergies

Crypto currencies and e-commerce?

Securing VoIP

Domain Names

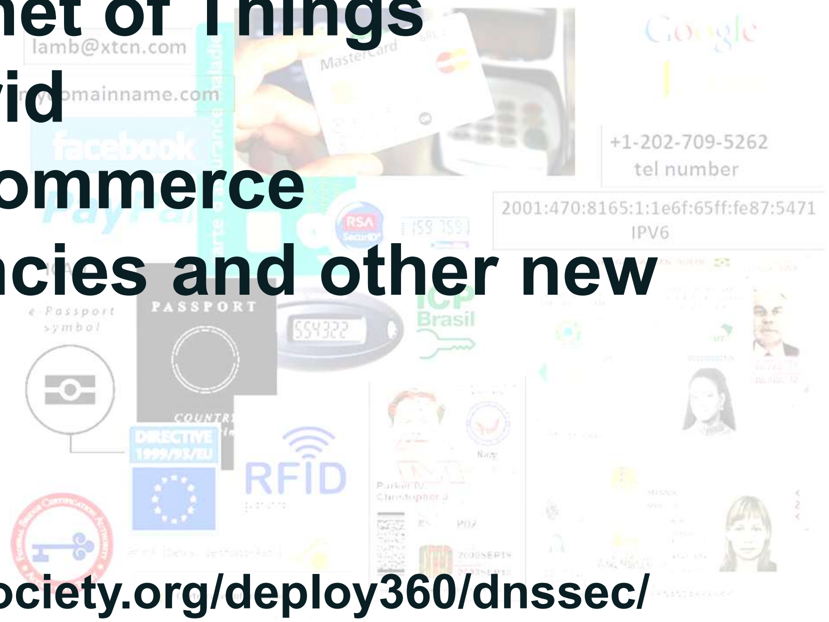
E-mail security SMIME,
DKIM RFC4871

Login security
SSHFP RFC4255

https://www.eff.org/observatory
http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/

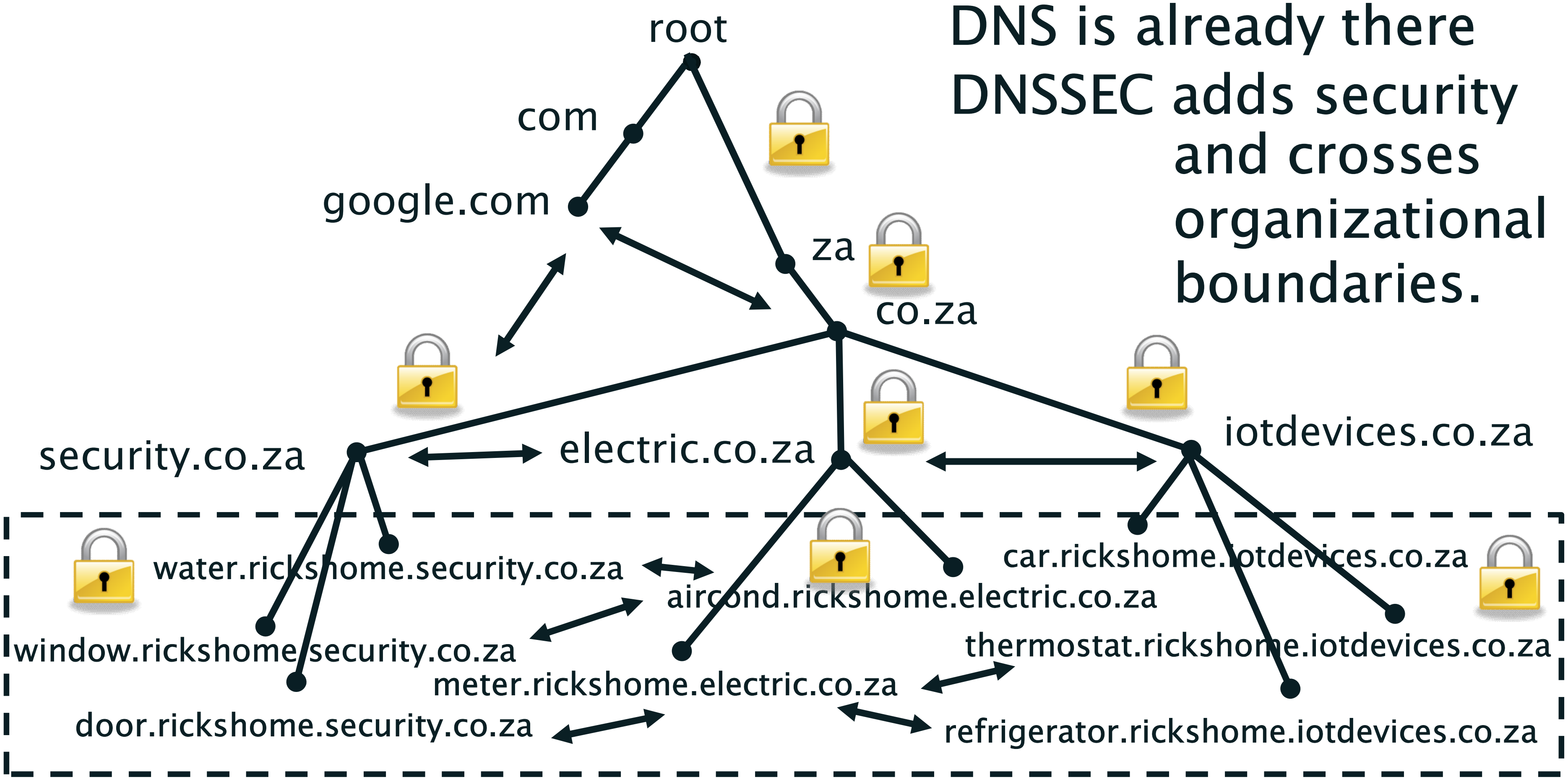
Opportunity: New Security Solutions

- **Improved Web SSL and certificates for all***
- **Secured e-mail (e.g., s/mime, pgp) for all***
- **Securing VoIP**
- **Cross organizational authentication+security**
- **Secured content delivery (e.g. configurations, updates, keys) – Internet of Things**
- **Securing the Smart Grid**
- **Increasing trust in e-commerce**
- **Securing cryptocurrencies and other new models**
- ***A Global Built-in PKI***



A good ref http://www.internetsociety.org/deploy360/dnssec/
***IETF standards complete and interest by govt procurement**

A thought: Scalable Security for IoT


root
com
google.com
za
co.za
security.co.za
electric.co.za
iotdevices.co.za
water.rickshome.security.co.za
window.rickshome.security.co.za
door.rickshome.security.co.za
aircond.rickshome.electric.co.za
meter.rickshome.electric.co.za
car.rickshome.iotdevices.co.za
thermostat.rickshome.iotdevices.co.za
refrigerator.rickshome.iotdevices.co.za

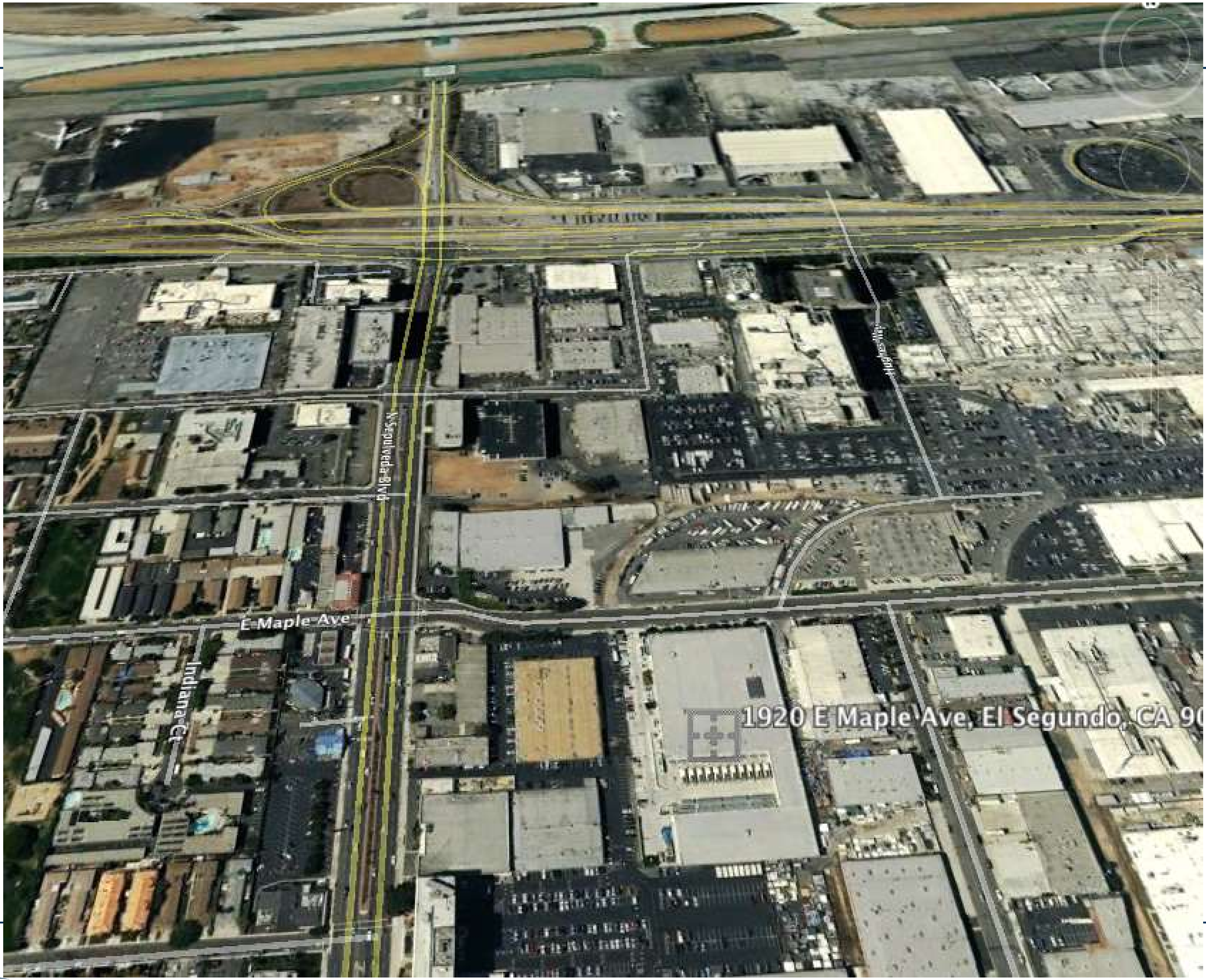
DNS is already there

DNSSEC adds security and crosses organizational boundaries.

Animated slide

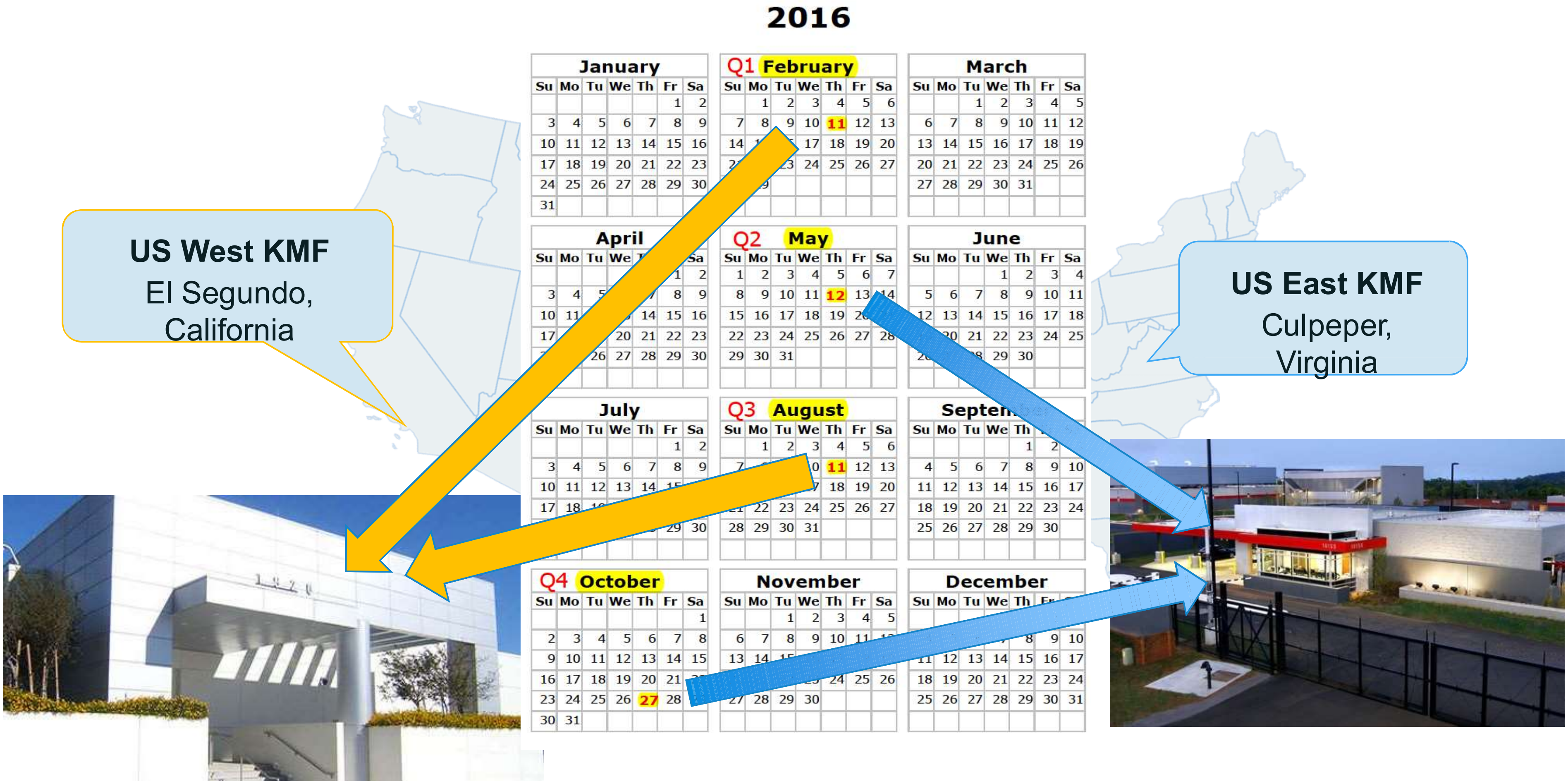
DNSSEC: Internet infrastructure upgrade to help address today’s needs and create tomorrow’s opportunity.

What Hollywood Sees – part 2


N Sepulveda Blvd
E Maple Ave
Indiana Ct
1920 E Maple Ave, El Segundo, CA 9

January 27, 2010

Key Management Facility (KMF)



US West KMF
El Segundo,
California

US East KMF
Culpeper,
Virginia

2016

January						
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Q1 February						
Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	**11**	12	13
14	15	[illegible]	17	18	19	20
21	[illegible]	23	24	25	26	27
[illegible]	29					

March						
Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

April						
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	[illegible]	7	8	9
10	11	[illegible]	13	14	15	16
17	[illegible]	[illegible]	20	21	22	23
24	[illegible]	26	27	28	29	30

Q2 May						
Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	**12**	13	14
15	16	17	18	19	20	[illegible]
22	23	24	25	26	27	28
29	30	31				

June						
Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
[illegible]	20	21	22	23	24	25
26	[illegible]	28	29	30		

July						
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	[illegible]
17	18	19	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	29	30

Q3 August						
Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	[illegible]	10	**11**	12	13
[illegible]	[illegible]	[illegible]	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

September						
Su	Mo	Tu	We	Th	Fr	Sa
				1	2	[illegible]
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Q4 October						
Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	**27**	28	[illegible]
30	31					

November						
Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	23	24	25	26
27	28	29	30			

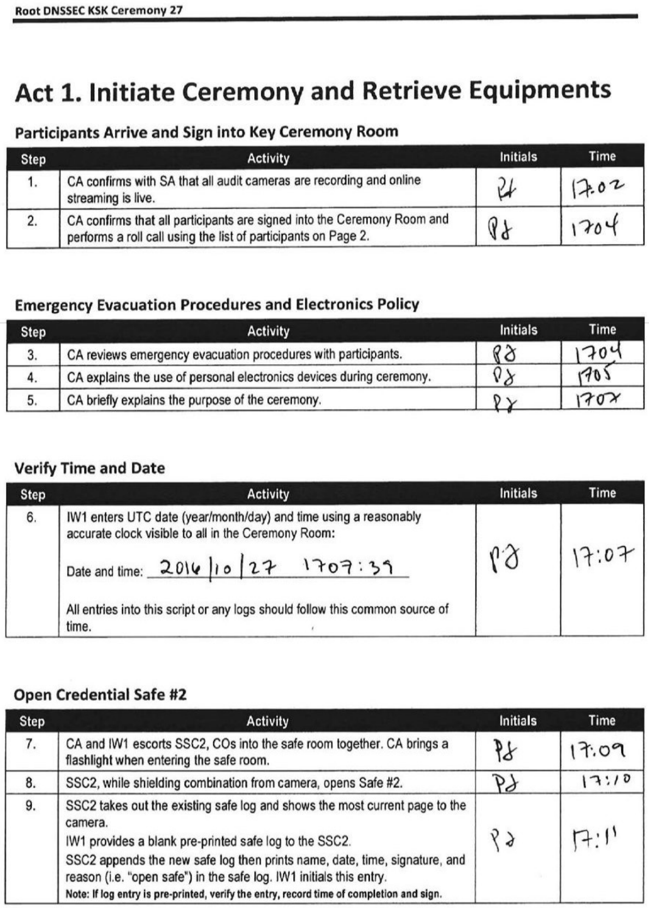
December						
Su	Mo	Tu	We	Th	Fr	Sa
				[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

~~Team Ceremony~~ Key Ceremony

~~Tea Ceremony~~

Not like this Ceremony

Key Ceremony



Root DNSSEC KSK Ceremony 27

Act 1. Initiate Ceremony and Retrieve Equipments

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are recording and online streaming is live.	PJ	17:02
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the list of participants on Page 2.	PJ	1704

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	PJ	1704
4.	CA explains the use of personal electronics devices during ceremony.	PJ	1705
5.	CA briefly explains the purpose of the ceremony.	PJ	1707

Verify Time and Date

Step	Activity	Initials	Time
6.	IW1 enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room: Date and time: 2016/10/27 1707:39 All entries into this script or any logs should follow this common source of time.	PJ	17:07

Open Credential Safe #2

Step	Activity	Initials	Time
7.	CA and IW1 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.	PJ	17:09
8.	SSC2, while shielding combination from camera, opens Safe #2.	PJ	17:10
9.	SSC2 takes out the existing safe log and shows the most current page to the camera. IW1 provides a blank pre-printed safe log to the SSC2. SSC2 appends the new safe log then prints name, date, time, signature, and reason (i.e. "open safe") in the safe log. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PJ	17:11

Photo by Kim Davies

Key Signing Ceremony

Trusted Community Representatives 🧍 🧍 🧍

Enable the HSMs

Ceremony Administrator 🧍

Performs the Ceremony using scripts

Internal Witness 🧍 🧍

Attests the ceremony, signs affidavit

Hardware Safe Controller 🧍

Opens Safe #1

Credential Safe Controller 🧍

Opens Safe #2

System Administrator 🧍

Technical Support and Evidence Collection

Third-Party Auditors 🧍 🧍

Observe and Attest

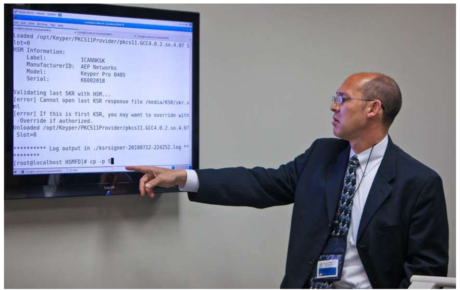
Root Zone Management Partner 🧍

Bring Key Signing Request

At least 12 people!

Minimum Participants

Photos



```
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 S
lot=0
HSM Information:
    Label:              ICANNKSK
    ManufacturerID:     AEP Networks
    Model:              Keyper Pro 0405
    Serial:             K6002018

Validating last SKR with HSM...
[error] Cannot open last KSR response file /media/KSR/skr.x
ml
[error] If this is first KSR, you may want to override with
 -Override if authorized.
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
 Slot=0

********** Log output in ./ksrsigner-20100712-224252.log **
********
[root@localhost HSMFD]# cp -p $
```

Photo: Kim Davies

Photo by Olaf Kolkman

Photo: www.dj.cx

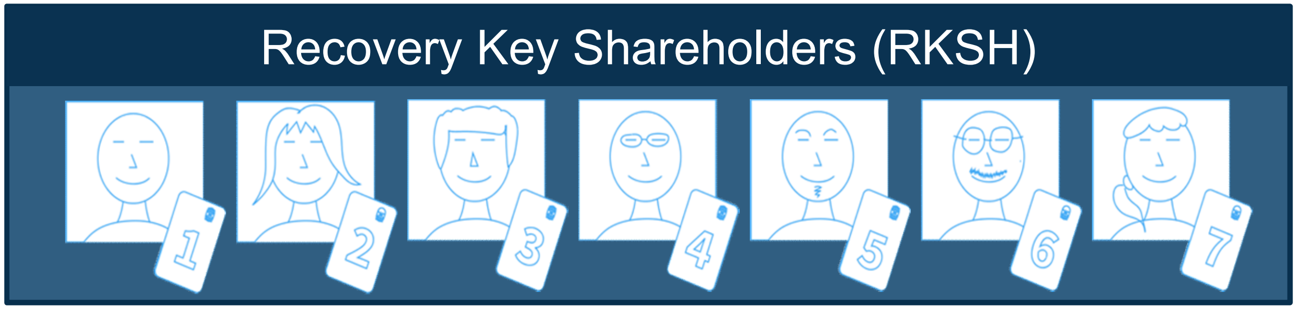
Photo: www.dj.cx

Photo: www.dj.cx

Photo: www.dj.cx

Photo: Kim Davies

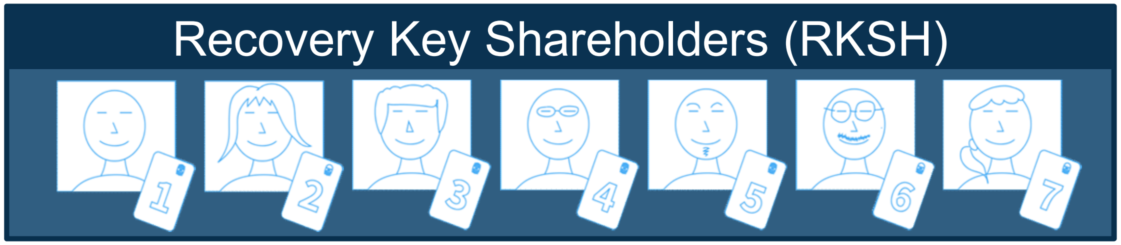
Trusted Community Representatives (TCRs)



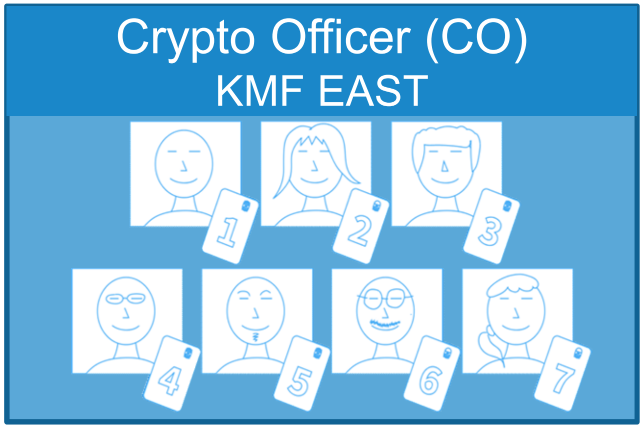
Recovery Key Shareholders (RKSH)

Photo: Kim Davies

Trusted Community Representatives (TCRs)

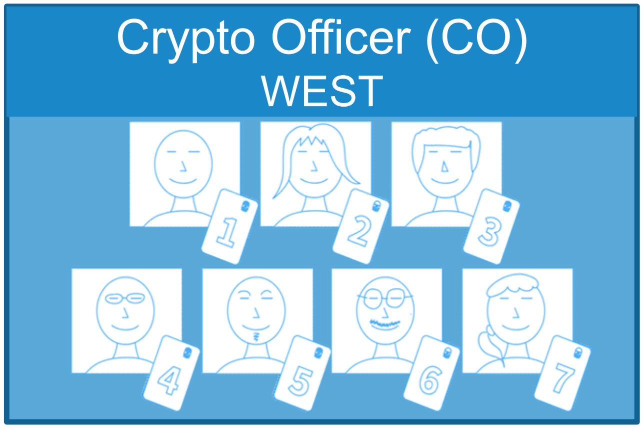


Recovery Key Shareholders (RKSH)



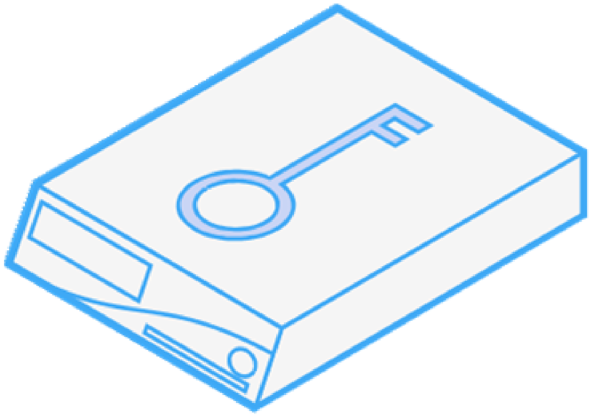
Crypto Officer (CO)
KMF EAST

21 TCRs!



Crypto Officer (CO)
WEST

Hardware Security Module (HSM)



FIPS 140-2 Level 4
Certified

Photo: www.dj.cx

- Private Key for KSK-2010
- Private Key for KSK-2017

Smart Cards

Smart Cards

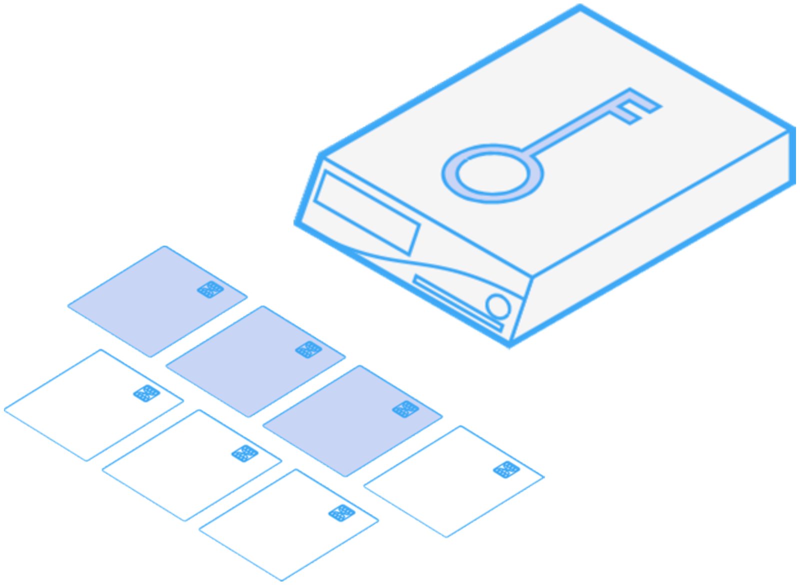
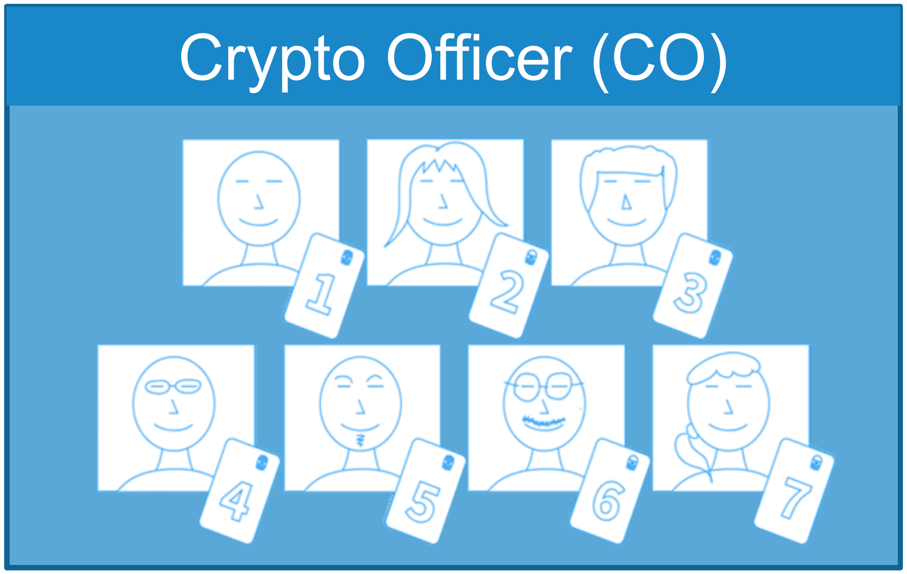


Photo: www.dj.cx

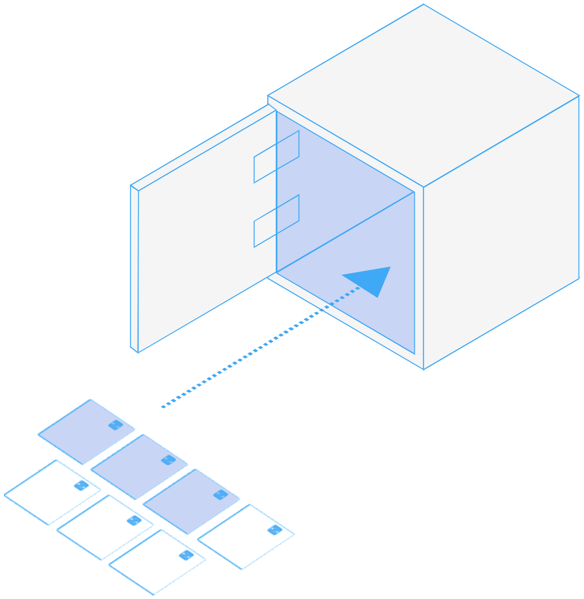
Trusted Community Representative (TCR)



Each smart card is assigned to different community members, known as **Trusted Community Representatives**

Photo by Kim Davies

Safe # 2 – Credential Safe



Smart Cards

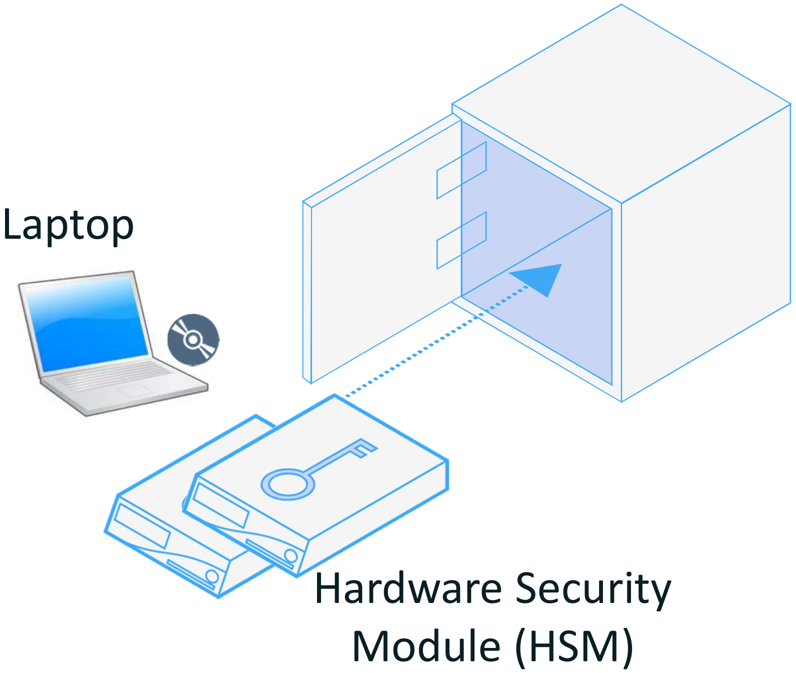
Photo: Olaf Kolkman

Photo: www.dj.cx

Can only be opened by a designated staff, **Credential Safe Controller**

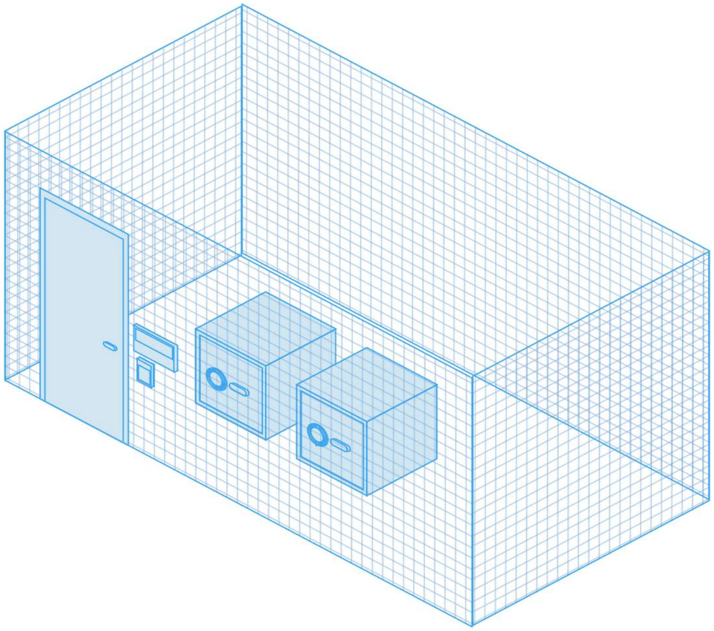
Safe #1 – Hardware Safe

Photo: www.dj.cx



Can only be opened by a designated staff,
Hardware Safe Controller

Safe Room



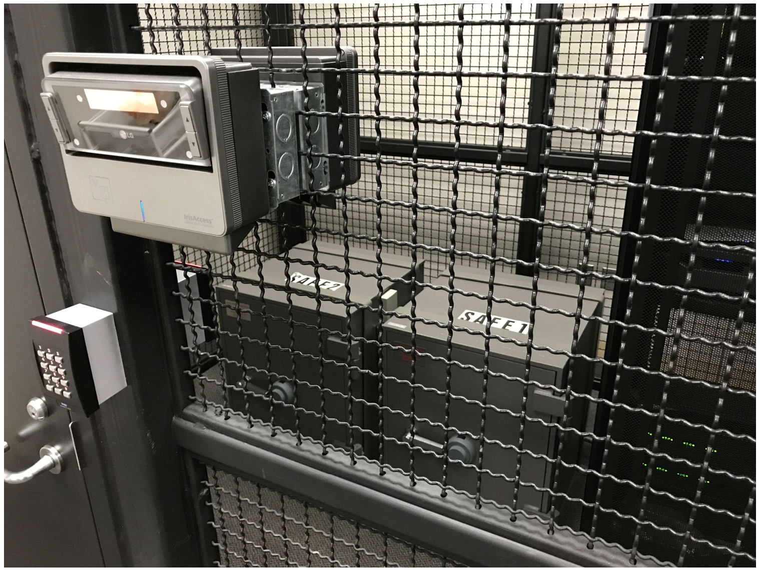


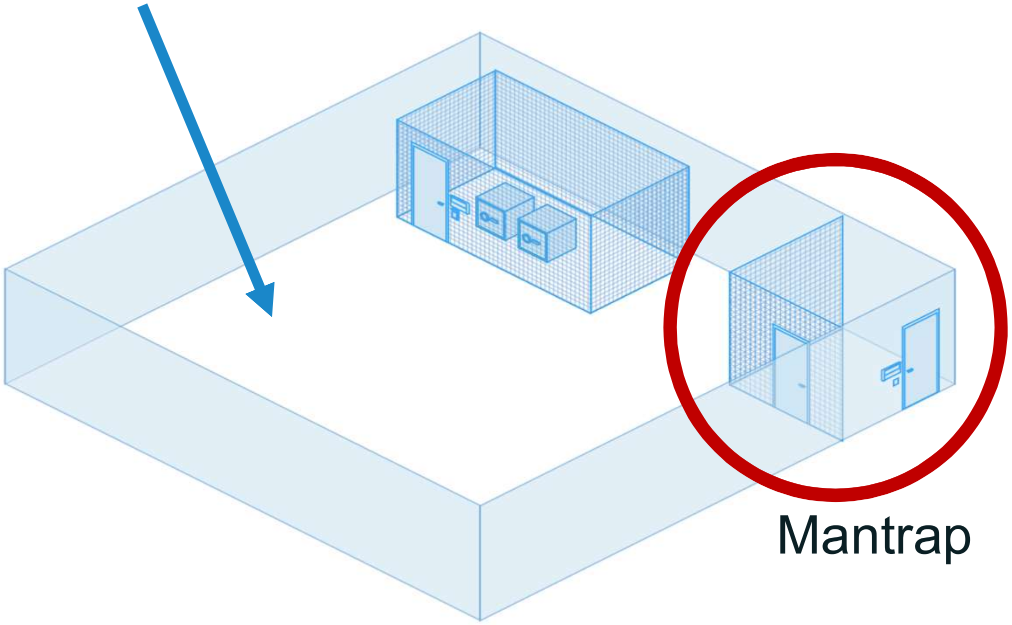
Photo: www.dj.cx

Photo: Kim Davies

Ceremony Room

8:55
NOTICE
NO CONCEALED WEAPONS BEYOND THIS POINT
NOTICE
ALL ACTIVITIES MONITORED BY VIDEO CAMERA

Photo: www.dj.cx



RESTRICTED AREA
AUTHORIZED PERSONNEL ONLY
NOTICE
NO CONCEALED WEAPONS BEYOND THIS POINT
NOTICE
NO FOOD OR DRINK BEYOND THIS POINT
WAIT
PROCEED
ICANN

SOC 3 Certification

AICPA Service Organization Control Reports
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports
®

NOTICE
NOTICE
UNAUTHORIZED PERSONS NOT PERMITTED
NOTICE
NO FOOD OR DRINK
3066
EXIT
One World. One Internet. Everyone Connected.
19036

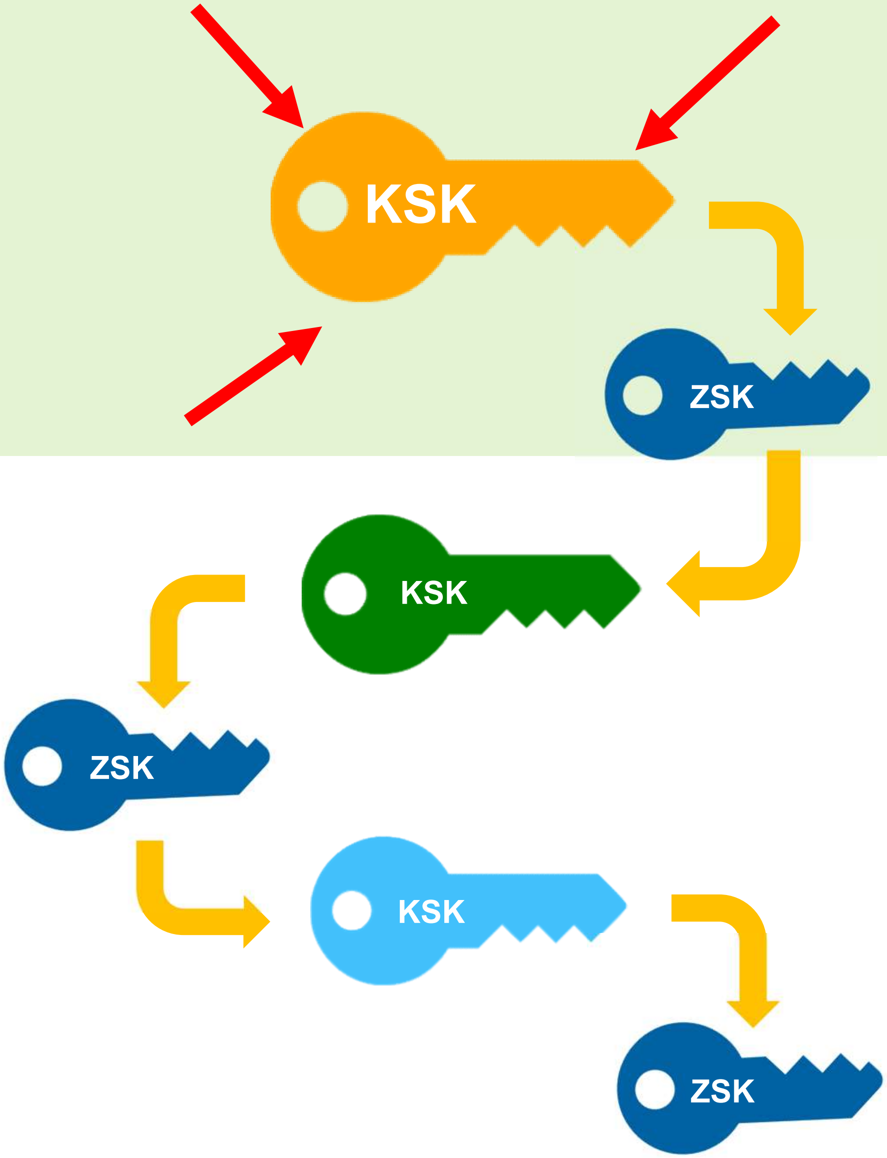
Photos: Kim Davies

- Working together there is hope to stem the tide of cybercrime
- One example is DNSSEC. This upgrade to the Internet’s core infrastructure will help address today’s problems and support tomorrow’s security solutions

Root Zone DNSSEC KSK Rollover

Root Zone DNSSEC KSK

The Root Zone DNSSEC Key Signing Key "**KSK**" is the top most cryptographic key in the DNSSEC hierarchy



DNSSEC = **"DNS Security Extensions"**

DNSSEC is a protocol that is currently being deployed to secure the Domain Name System (DNS)

Root Zone DNSSEC KSK Rollover

RSA-2048

Old Key called **KSK-2017**
(Operational)

RSA-2048

New Key called **KSK-2017**

Root Zone DNSSEC KSK – KSK-2017

```
. IN DNSKEY  257 3 8
        AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
        +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
        ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
        0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
        oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
        RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
        R1AkUTV74bU=
```

How To Update Your System

If your software supports automated updates of DNSSEC trust anchors (RFC 5011):

- The KSK will be updated automatically at the appropriate time
- You do not need to take additional action
  - Devices that are offline during the rollover will have to be updated manually if they are brought online after the rollover is finished

If your software does <u>not</u> support automated updates of DNSSEC trust anchors (RFC 5011) or is not configured to use it:

- The software's trust anchor file must be manually updated
- The new root zone KSK is now available here after March 2017:

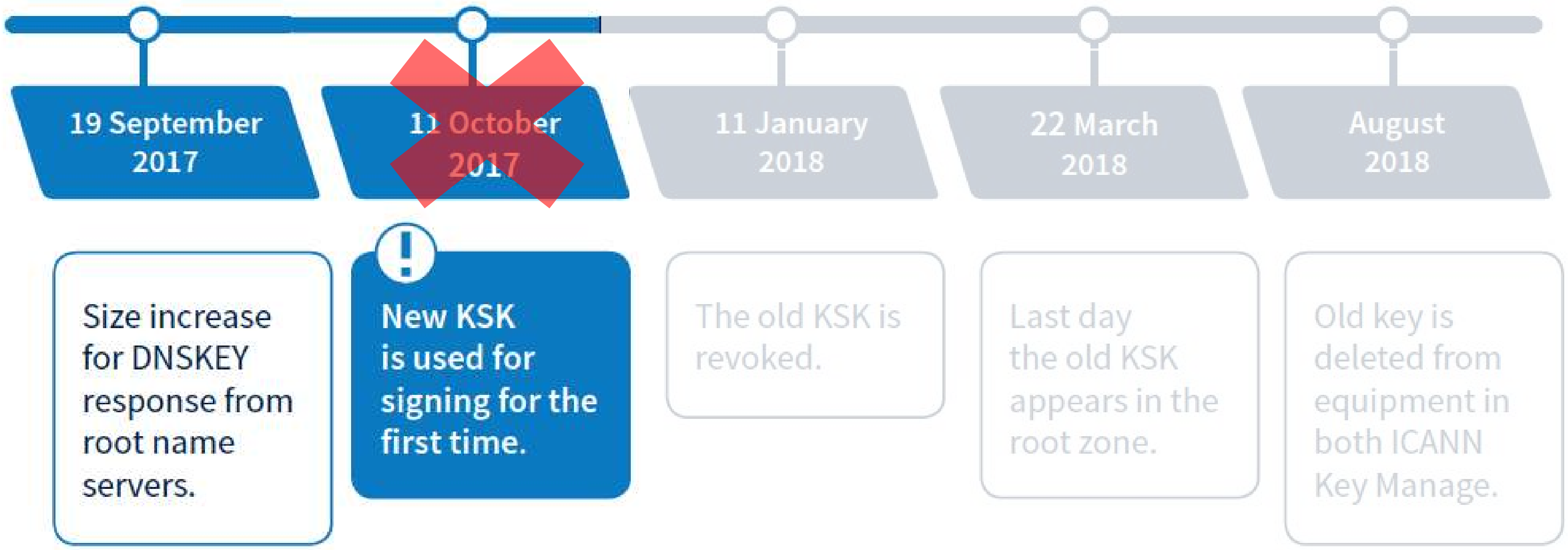
Root Anchors ▶

data.iana.org/root-anchors

When Does the Rollover Take Place?

The KSK rollover is a process, not a single event

The following dates are key milestones in the process when end users may experience interruption in Internet services:



19 September 2017

Size increase for DNSKEY response from root name servers.

~~11 October 2017~~

!

New KSK is used for signing for the first time.

11 January 2018

The old KSK is revoked.

22 March 2018

Last day the old KSK appears in the root zone.

August 2018

Old key is deleted from equipment in both ICANN Key Manage.

Check to See If Your Systems Are Ready

ICANN is offering a **test bed** for operators or any interested parties to confirm that their systems handle the automated update process correctly.

Check to make sure your systems are ready by visiting:
go.icann.org/KSKtest

Thank You

Email: richard.lamb@icann.org

I had help and material from many.
Special thanks to:
Punky Duero

youtube.com/icannnews

linkedin/company/icann

www.icann.org

ICANN provided KSK Rollover Information and Tools:

https://www.icann.org/kskroll

https://github.com/iana-org/get-trust-anchor
https://go.icann.org/KSKtest

Root Zone DNSSEC Trust Anchor:

https://data.iana.org/root-anchors

Call for TCRs:

https://www.iana.org/help/tcr-application