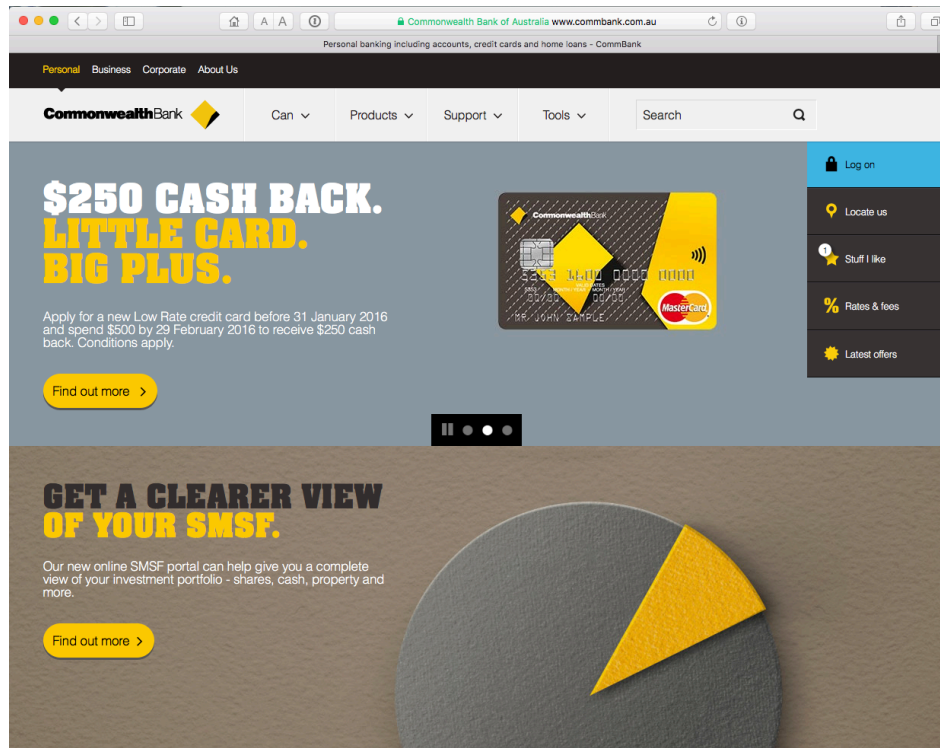


Why Dane?

Geoff Huston
Chief Scientist, APNIC

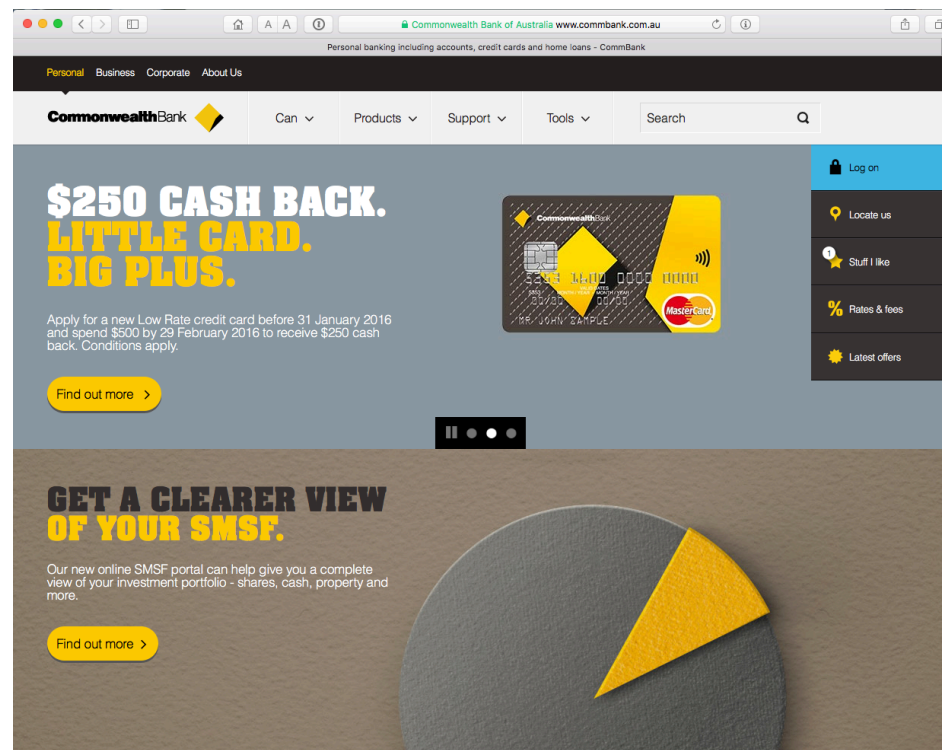
Which Bank? My Bank!



I hope!

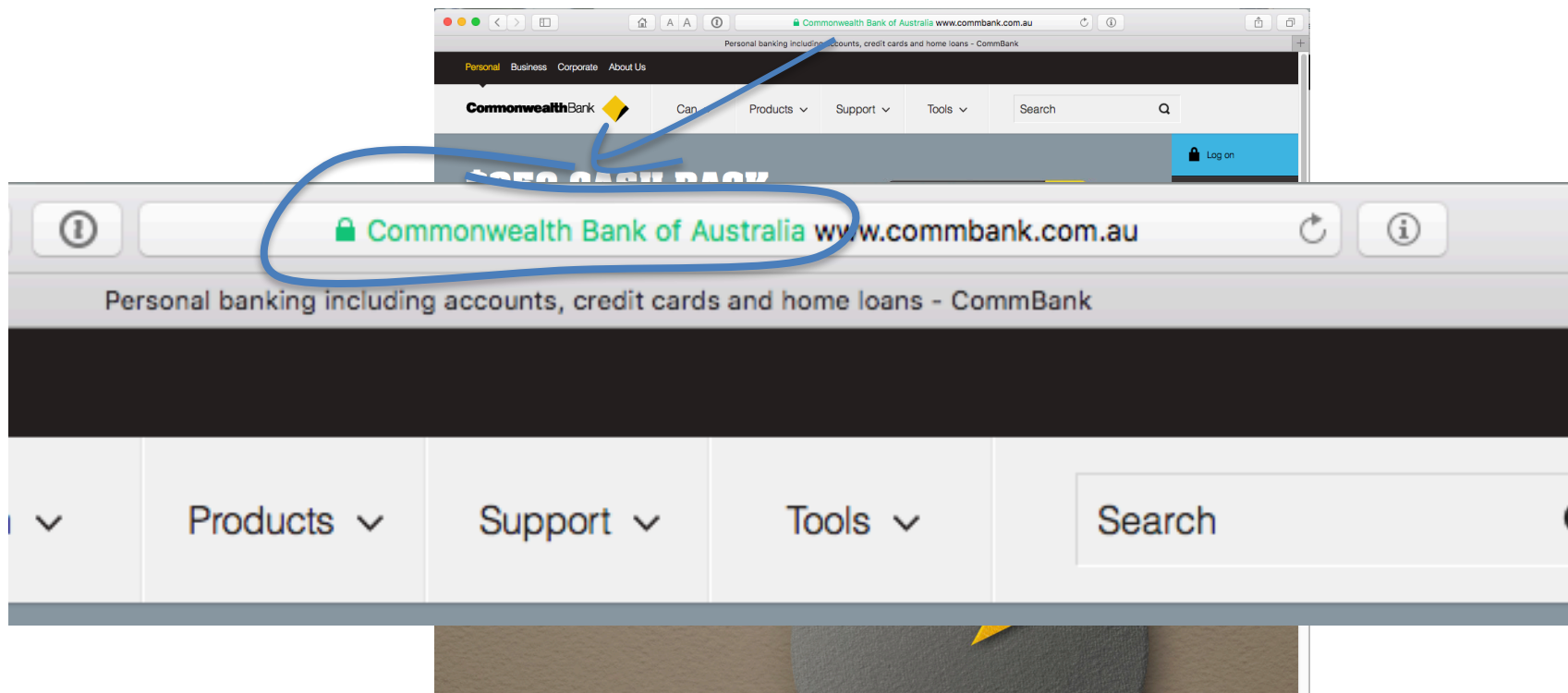
Security on the Internet

How do you know that you are going to where you thought you were going to?



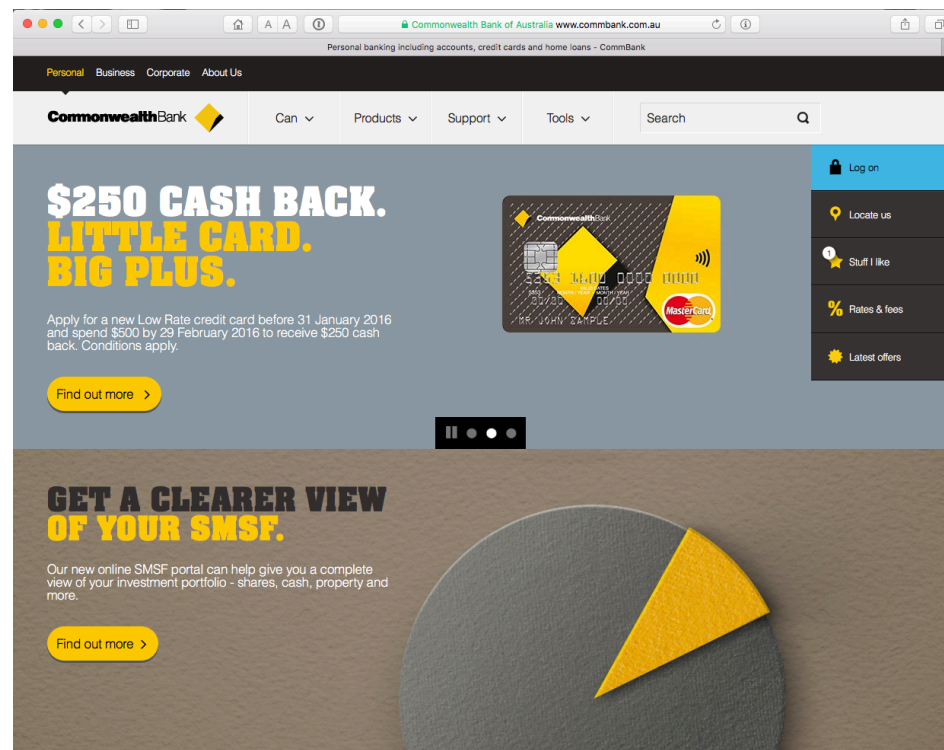
Security on the Internet

How do you know that you are going to where you thought you were going to?



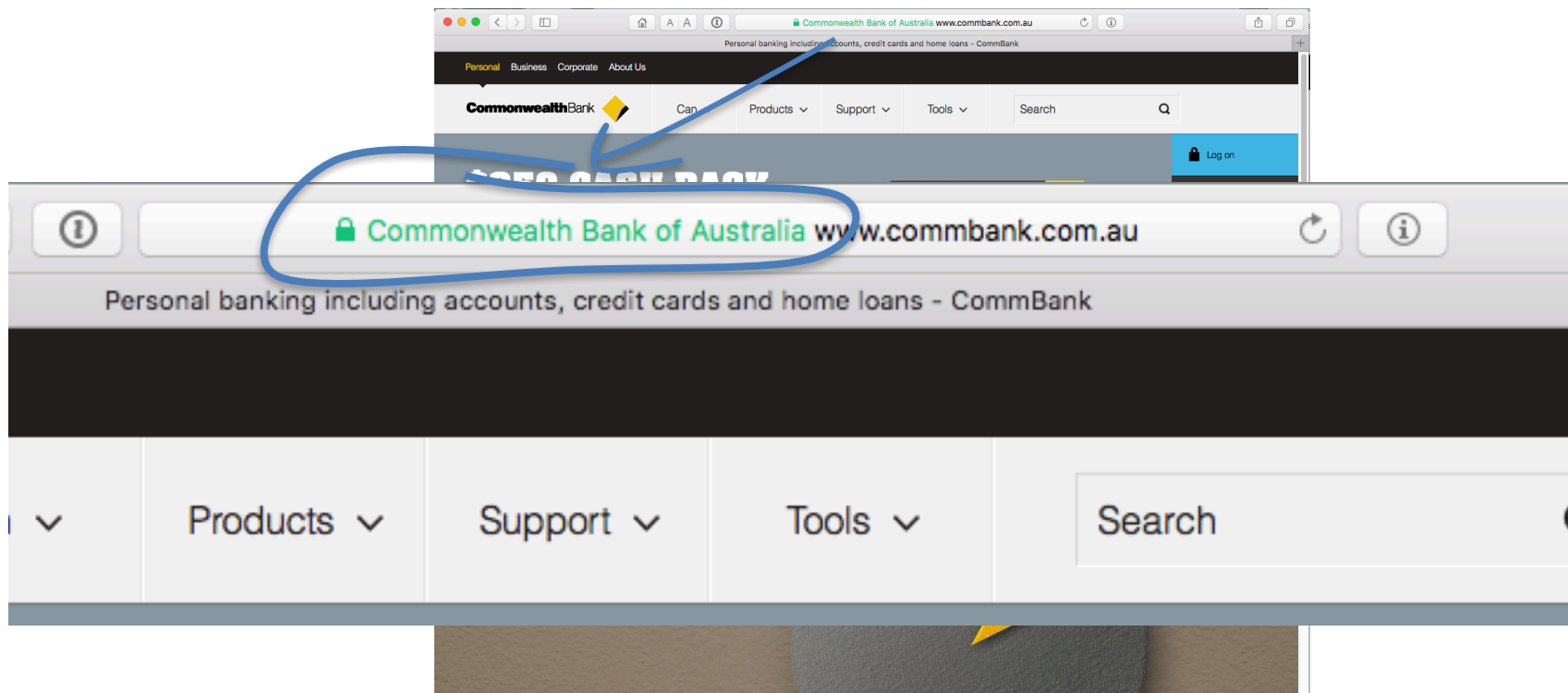
Security on the Internet

Also, how can you keep your session a secret from wire(less) snoopers?



Security on the Internet

Also, how can you keep your session a secret from wire(less) snoopers?



Opening the Connection: First Steps



Client:

DNS Query:

www.commbank.com.au?



DNS Response:

104.97.235.12

TCP Session:

TCP Connect 104.97.235.12, port 443



Hang on...

```
$ dig -x 104.97.235.12 +short  
a104-97-235-12.deploy.static.akamaitechnologies.com.
```

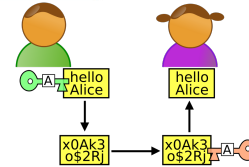
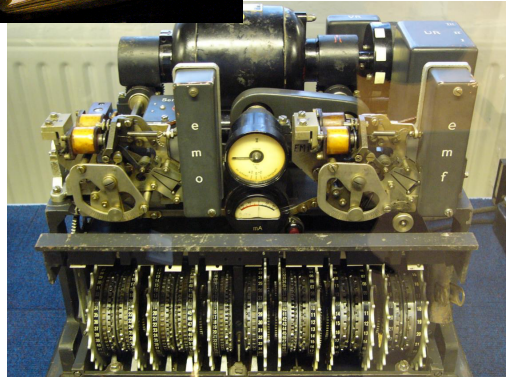
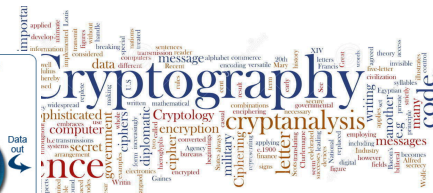
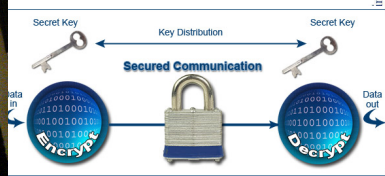
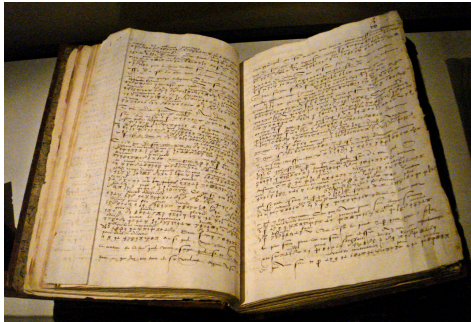
That's **not** an IP addresses that was allocated to the Commonwealth Bank!

The Commonwealth Bank of Australia has 140.168.0.0 - 140.168.255.255
and 203.17.185.0 - 203.17.185.255

So why should my browser trust that 104.97.235.12 is really the “proper” web site for the Commonwealth Bank of Australia, and not some dastardly evil scam designed to steal my passwords and my money?

How can my browser tell the difference between an intended truth and a lie?

Its all about cryptography



The Basic Challenge

Pick a pair of keys such that:

- Messages encoded with one key can only be decoded with the other key
- Knowledge of the value of one key does not infer the value of the other key



The Power of Primes

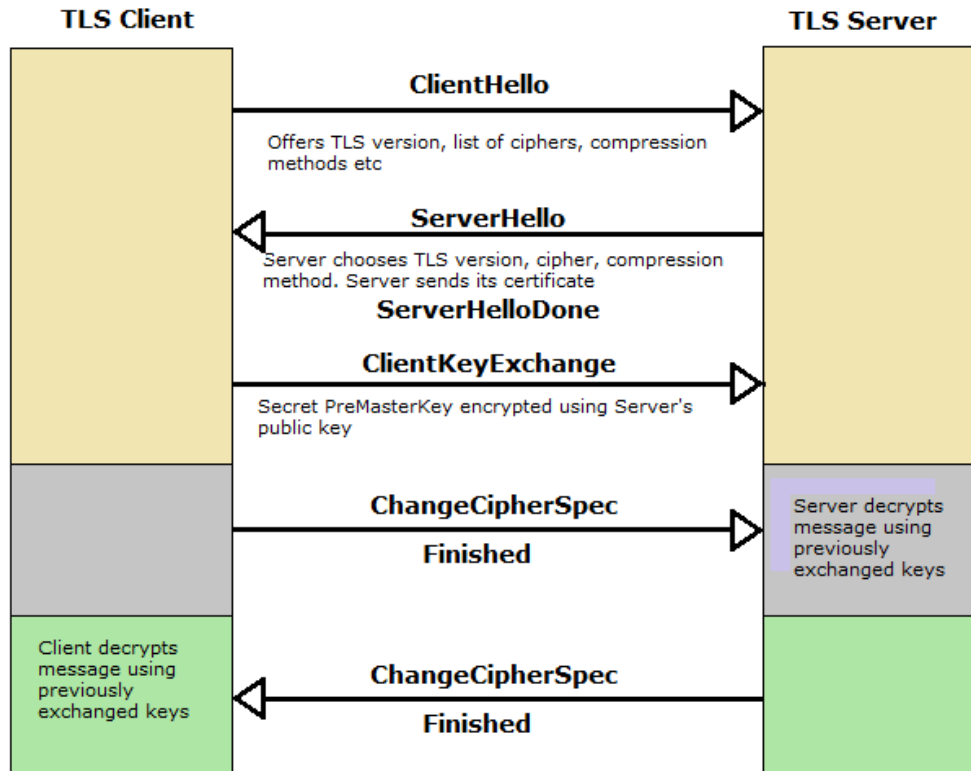
$$(m^e)^d \equiv m \pmod{n}$$

As long as d and n are relatively large, and n is the product of two large prime numbers, then finding the value of d when you already know the values of e and n is computationally expensive

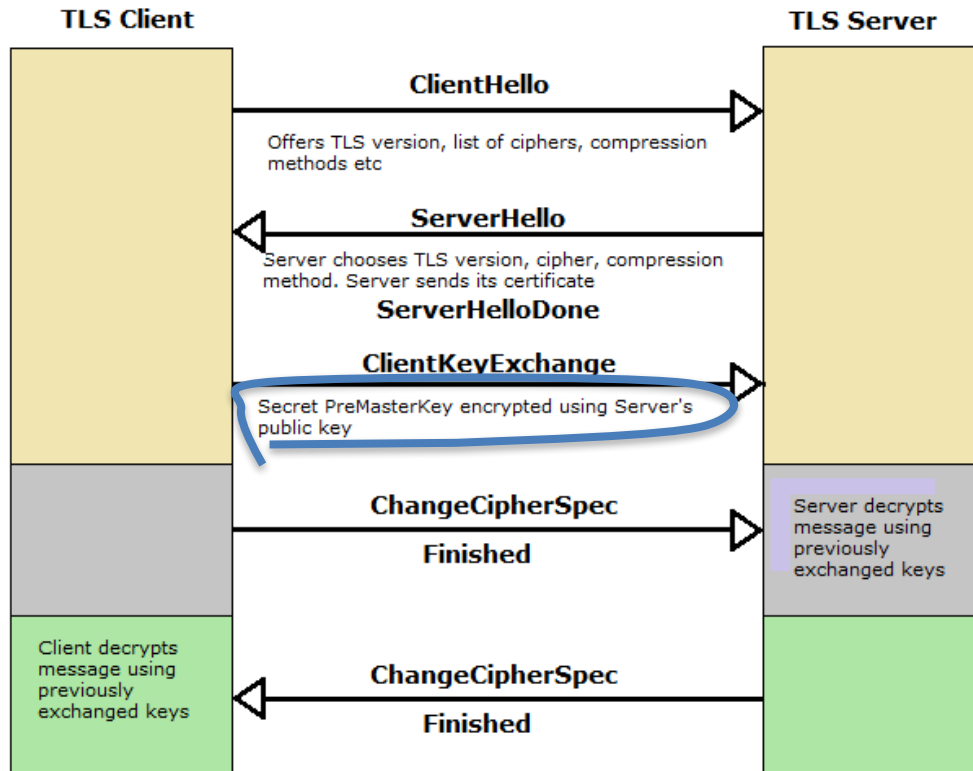
Why is this important?

Because much of the
foundation of internet
Security rests upon this
prime number relationship

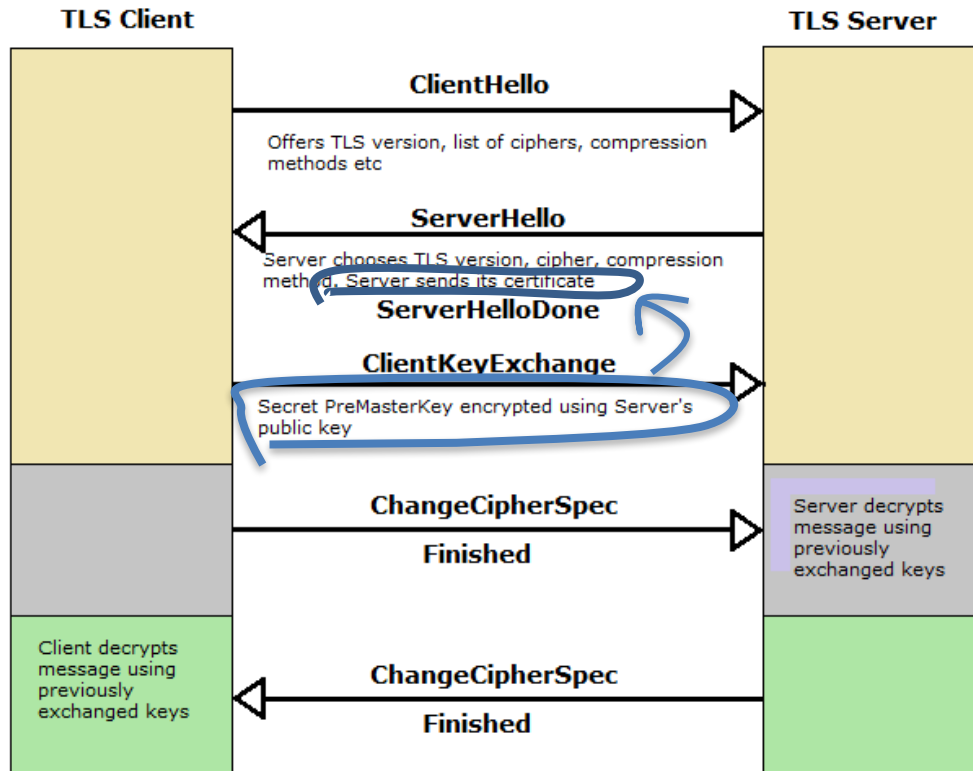
TLS Connections



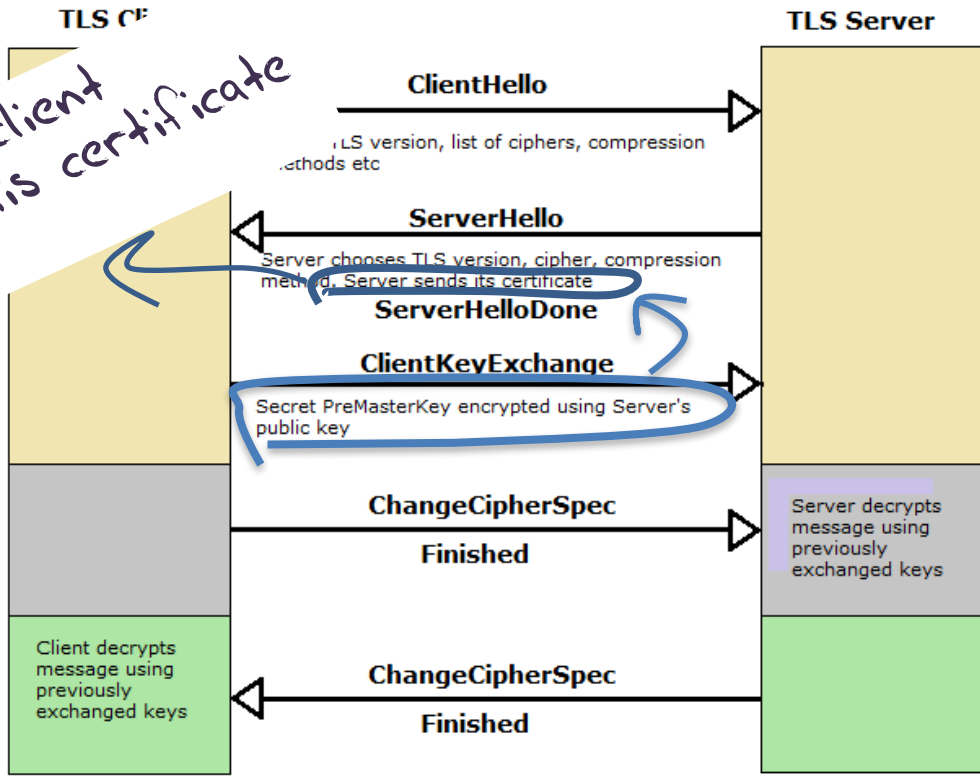
TLS Connections



TLS Connections



TLS Connections



How does the client "recognise" this certificate as valid?



Safari is using an encrypted connection to www.commbank.com.au.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.commbank.com.au.

Symantec Corporation has identified www.commbank.com.au as being owned by Commonwealth Bank of Australia in SYDNEY, New South Wales, AU.

- VeriSign Class 3 Public Primary Certification Authority - G5
- Symantec Class 3 EV SSL CA - G3
- www.commbank.com.au



www.commbank.com.au

Issued by: Symantec Class 3 EV SSL CA - G3
Expires: Saturday, 27 February 2016 at 10:59:59 AM Australian Eastern Daylight Time
This certificate is valid

- Trust
- Details

Subject Name	
Inc. Country	AU
Business Category	Private Organization
Serial Number	123 123 124
Country	AU
Postal Code	2000
State/Province	New South Wales
Locality	SYDNEY
Street Address	201 SUSSEX S T
Organization	Commonwealth Bank of Australia
Organizational Unit	CBA Business System Hosting
Common Name	www.commbank.com.au
Issuer Name	
Country	US
Organization	Symantec Corporation
Organizational Unit	Symantec Trust Network
Common Name	Symantec Class 3 EV SSL CA - G3
Serial Number	1A 9F E9 4B 03 9D E2 9A B6 15 56 69 60 3E 98 AE
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Not Valid Before	Monday, 4 May 2015 at 10:00:00 AM Australian Eastern Standard Time
Not Valid After	Saturday, 27 February 2016 at 10:59:59 AM Australian Eastern Daylight Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : CA B4 74 93 E8 00 22 10 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	256 bytes : 95 32 C3 F0 62 F1 F8 F1 ...



Hide Certificate

OK

Log on

Locate us

Stuff I like

Rates & fees

Latest offers

GET A C
OF YOU

Our new online SMSF
view of your investme
more.

Find out more >

FAMILIAR BANKING
FOR UNFAMILIAR



Safari is using an encrypted connection to www.commbank.com.au.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.commbank.com.au.

Symantec Corporation has identified www.commbank.com.au as being owned by Commonwealth Bank of Australia in SYDNEY, New South Wales, AU.

VeriSign Class 3 Public Primary Certification Authority - G5

Symantec Class 3 EV SSL CA - G3

www.commbank.com.au



www.commbank.com.au

Issued by: Symantec Class 3 EV SSL CA - G3
Expires: Saturday, 27 February 2016 at 10:59:59 AM Australian Eastern Daylight Time

✓ This certificate is valid

- ▶ Trust
- ▼ Details

Subject Name	
Inc. Country	AU
Business Category	Private Organization
Serial Number	123 123 124
Country	AU
Postal Code	2000
State/Province	New South Wales
Locality	SYDNEY
Street Address	201 SUSSEX S T
Organization	Commonwealth Bank of Australia
Organizational Unit	CBA Business System Hosting
Common Name	www.commbank.com.au
Issuer Name	
Country	US
Organization	Symantec Corporation
Organizational Unit	Symantec Trust Network
Common Name	Symantec Class 3 EV SSL CA - G3
Serial Number	1A 9F E9 4B 03 9D E2 9A B6 15 56 69 60 3E 98 AE
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Not Valid Before	Monday, 4 May 2015 at 10:00:00 AM Australian Eastern Standard Time
Not Valid After	Saturday, 27 February 2016 at 10:59:59 AM Australian Eastern Daylight Time

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : CA B4 74 93 E8 00 22 10 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	256 bytes : 95 32 C3 F0 62 F1 F8 F1 ...

How did my browser know that this is a valid cert?



Hide Certificate

OK

Log on

Locate us

Stuff I like

Rates & fees

Latest offers

GET A C OF YOU

Our new online SMSF view of your investments more.

Find out more >

FAMILIAR BANKING FOR UNFAMILIAR

Domain Name Certification

- The Commonwealth Bank of Australia has generated a key pair
- And they passed a certificate signing request to a company called “Symantec”
- Who is willing to vouch (in a certificate) that the entity who goes by the domain name of www.commbank.com.au also has a certain public key value
- So if I can associate this public key with a connection then I have a high degree of confidence that I’ve connected to www.commbank.com.au, as long as I am prepared to trust Symantec and the certificates that they issue

Domain Name Certification

- The Commonwealth Bank of Australia has generated a key pair
- And they passed a certificate signing request to a company called “Symantec”
- Who is willing to vouch (in a certificate) that the entity who goes by the domain name of www.commbank.com.au also has a certain public key value
- So if I can associate this public key with a connection then I have a high degree of confidence that I’ve connected to www.commbank.com.au, as long as I am prepared to trust Symantec and the certificates that they issue

Why should i trust them?

Local Trust

Click to unlock the System Roots keychain.

Keychains

- login
- Directory Services
- iCloud
- System
- System Roots

Category

- All Items

AAA Certificate Services

Root certificate authority
Expires: Monday, 1 January 2029 at 10:59:59 AM Australian Eastern Daylight Time
This certificate is valid

Name	Kind	Expires	Keychain
SwissSign Platinum Root CA - G2	certificate	25 Oct 2036, 7:36:00 PM	System Roots
SwissSign Platinum Root CA - G3	certificate	4 Aug 2037, 11:34:04 PM	System Roots
SwissSign Silver CA - G2	certificate	25 Oct 2036, 7:32:46 PM	System Roots
SwissSign Silver Root CA - G3	certificate	4 Aug 2037, 11:19:14 PM	System Roots
Symantec Class 1 Public Primary Certification Authority - G4	certificate	19 Jan 2038, 10:59:59 AM	System Roots
Symantec Class 1 Public Primary Certification Authority - G6	certificate	2 Dec 2037, 10:59:59 AM	System Roots
Symantec Class 2 Public Primary Certification Authority - G4	certificate	19 Jan 2038, 10:59:59 AM	System Roots
Symantec Class 2 Public Primary Certification Authority - G6	certificate	2 Dec 2037, 10:59:59 AM	System Roots
Symantec Class 3 Public Primary Certification Authority - G4	certificate	2 Dec 2037, 10:59:59 AM	System Roots
Symantec Class 3 Public Primary Certification Authority - G6	certificate	2 Dec 2037, 10:59:59 AM	System Roots
T-TeleSec GlobalRoot Class 2	certificate	2 Oct 2033, 10:59:59 AM	System Roots
T-TeleSec GlobalRoot Class 3	certificate	2 Oct 2033, 10:59:59 AM	System Roots
TC TrustCenter Class 2 CA II	certificate	1 Jan 2026, 9:59:59 AM	System Roots
TC TrustCenter Class 3 CA II	certificate	1 Jan 2026, 9:59:59 AM	System Roots
TC TrustCenter Class 4 CA II	certificate	1 Jan 2026, 9:59:59 AM	System Roots
TC TrustCenter Universal CA I	certificate	1 Jan 2026, 9:59:59 AM	System Roots
TC TrustCenter Universal CA II	certificate	1 Jan 2031, 9:59:59 AM	System Roots
TC TrustCenter Universal CA III	certificate	1 Jan 2030, 10:59:59 AM	System Roots
TeliaSonera Root CA v1	certificate	18 Oct 2032, 11:00:50 PM	System Roots
thawte Primary Root CA	certificate	17 Jul 2036, 9:59:59 AM	System Roots
thawte Primary Root CA - G2	certificate	19 Jan 2038, 10:59:59 AM	System Roots
thawte Primary Root CA - G3	certificate	2 Dec 2037, 10:59:59 AM	System Roots
TRUST2408 OCES Primary CA	certificate	4 Dec 2037, 12:11:34 AM	System Roots
Trusted Certificate Services	certificate	1 Jan 2029, 10:59:59 AM	System Roots
Trustis FPS Root CA	certificate	21 Jan 2024, 10:36:54 PM	System Roots
TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3	certificate	21 Aug 2017, 9:37:07 PM	System Roots
TÜRKRUST Elektronik Sertifika Hizmet Sağlayıcısı	certificate	23 Dec 2017, 5:37:19 AM	System Roots
TWCA Global Root CA	certificate	1 Jan 2031, 2:59:59 AM	System Roots
TWCA Root Certification Authority	certificate	1 Jan 2031, 2:59:59 AM	System Roots
UCA Global Root	certificate	31 Dec 2037, 11:00:00 AM	System Roots
UCA Root	certificate	31 Dec 2029, 11:00:00 AM	System Roots
UTN - DATACorp SGC	certificate	25 Jun 2019, 5:06:30 AM	System Roots
UTN - USERFirst - Client Authentication and Email	certificate	10 Jul 2019, 3:36:58 AM	System Roots
UTN - USERFirst - Hardware	certificate	10 Jul 2019, 4:19:22 AM	System Roots
UTN - USERFirst - Network Applications	certificate	10 Jul 2019, 4:57:49 AM	System Roots
UTN - USERFirst - Object	certificate	10 Jul 2019, 4:40:36 AM	System Roots
VeriSign Class 1 Public Primary Certification Authority - G3	certificate	17 Jul 2036, 9:59:59 AM	System Roots
VeriSign Class 2 Public Primary Certification Authority - G3	certificate	17 Jul 2036, 9:59:59 AM	System Roots
VeriSign Class 3 Public Primary Certification Authority - G3	certificate	17 Jul 2036, 9:59:59 AM	System Roots
VeriSign Class 3 Public Primary Certification Authority - G4	certificate	19 Jan 2038, 10:59:59 AM	System Roots
VeriSign Class 3 Public Primary Certification Authority - G5	certificate	17 Jul 2036, 9:59:59 AM	System Roots
VeriSign Class 4 Public Primary Certification Authority - G3	certificate	17 Jul 2036, 9:59:59 AM	System Roots
VeriSign Universal Root Certification Authority	certificate	2 Dec 2037, 10:59:59 AM	System Roots
Visa eCommerce Root	certificate	24 Jun 2022, 10:16:12 AM	System Roots
Visa Information Delivery Root CA	certificate	30 Jun 2025, 3:42:42 AM	System Roots
VRK Gov. Root CA	certificate	19 Dec 2023, 12:51:08 AM	System Roots
WellsSecure Public Root Certificate Authority	certificate	14 Dec 2022, 11:07:54 AM	System Roots
XRamp Global Certification Authority	certificate	1 Jan 2035, 4:37:19 PM	System Roots

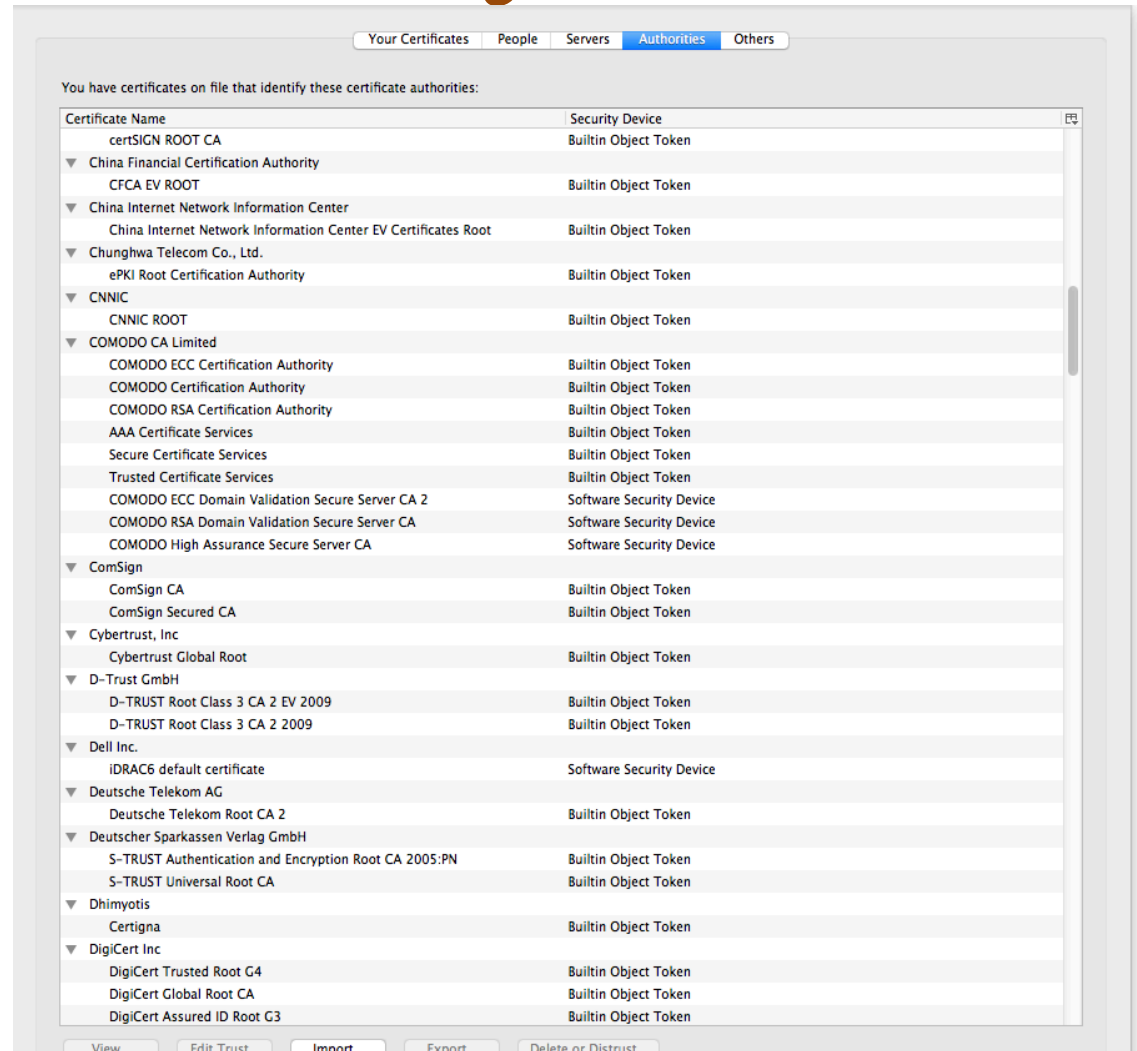
181 items

The cert I'm being asked to trust was issued by a certification authority that my browser already trusts - so I trust that cert!

Local Trust or Local Credulity*?

That's a big list of people to Trust

Are they all trustable?



* cre·du·li·ty

/krə'd(y)ooledē/

noun

a tendency to be too ready to believe that something is real or true.

Local Credulity

That's a big list of people to Trust

Are they all trustable?

Evidently Not!

The screenshot shows a web browser window with a tab titled "googleonlinesecurity.blogspot.com.au/2015/03/maint...". The browser's address bar shows the URL "googleonlinesecurity.blogspot.com.au/2015/03/maint...". The page content includes a navigation menu with tabs: "Your Certificates", "People", "Servers", "Authorities", and "Others". Below the navigation menu, there is a table with columns "Certificate Name" and "Security Device". The table lists various certificate authorities, including "certSIGN ROOT CA", "China Financial Certification Authority", "CFCA EV ROOT", "China Internet Network Information Center", "China Internet Network Information Center EV Certificates Root", "Chunghwa Telecom", "ePKI Root Certif", "CNNIC", "CNNIC ROOT", "COMODO CA Limit", "COMODO ECC C", "COMODO Certif", "COMODO RSA C", "AAA Certificate", "Secure Certifica", "Trusted Certific", "COMODO ECC I", "COMODO RSA I", "COMODO High", "ComSign", "ComSign CA", "ComSign Secur", "Cybertrust, Inc", "Cybertrust Glob", "D-Trust GmbH", "D-TRUST Root I", "D-TRUST Root I", "Dell Inc.", "IDRAC6 default", "Deutsche Telekom", "Deutsche Telek", "Deutscher Sparkas", "S-TRUST Authe", "S-TRUST Univer", "Dhimyotis", "Certigna", "DigiCert Inc", "DigiCert Truste", "DigiCert Global", and "DigiCert Assure". A blue circle highlights the "CNNIC" entry in the list. Below the table, there is a section titled "Maintaining digital certificate security" with a "Posted: Monday, March 23, 2015" date and social media sharing icons for Google+, Twitter, and Facebook. The post is by Adam Langley, Security Engineer. The main text of the post discusses unauthorized digital certificates for several Google domains, mentioning that the certificates were issued by an intermediate certificate authority held by a company called MCS Holdings, and that this intermediate certificate was issued by CNNIC. A blue circle highlights the sentence: "CNNIC is included in all major root stores and so the misissued certificates would be trusted by almost all browsers and operating systems. Chrome on Windows, OS X, and Linux, ChromeOS, and Firefox 33 and greater would have rejected these certificates because of public-key pinning, although misissued certificates for other sites likely exist." Below this, the post continues to describe the incident, mentioning that the author promptly alerted CNNIC and other major browsers about the incident, and that they blocked the MCS Holdings certificate in Chrome with a CRLSet push. CNNIC responded on the 22nd to explain that they had contracted with MCS Holdings on the basis that MCS would only issue certificates for domains that they had registered. However, rather than keep the private key in a suitable HSM, MCS installed it in a man-in-the-middle proxy. These devices intercept secure connections by masquerading as the intended destination and are sometimes used by companies to intercept their employees' secure traffic for monitoring or legal reasons. The employees' computers normally have to be configured to trust a proxy for it to be able to do this. However, in this case, the presumed proxy was given the full authority of a public CA, which is a serious breach of the CA system. This situation is similar to a failure by ANSSI in 2013.

Local Credulity

That's a big list of people to Trust

Are they all trustable?

Evidently Not!

The screenshot shows a Windows Certificate Manager window with the 'Authorities' tab selected. A list of certificate authorities is displayed, with 'COMODO CA Limited' circled in blue. An arrow points from this circled name to the article title 'The real security issue behind the Comodo hack' in the InfoWorld article. The article text includes: 'News of an Iranian hacker duping certification authority Comodo into issuing digital certificates to one or more unauthorized parties has caused an uproar in the IT community, moving some critics to call for Microsoft and Mozilla to remove Comodo as a trusted root certification authority from the systems under their control. Though the hacker managed his feat by first compromising a site containing a hard-coded logon name and password, then generating certificates for several well-known sites, including Google, Live.com, Skype, and Yahoo, I'm not bothered by the...'

But my bank used Symantec

as their Certificate Authority

And Symantec NEVER lie in the certificates they issue

Never?

Well, hardly ever

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

Already on probation, Symantec issues more illegit HTTPS certificates

At least 108 Symantec certificates threatened the integrity of the encrypted Web.

DAN GOODIN - 1/21/2017, 8:40 AM



Enlarge

62

A security researcher has unearthed evidence showing that three browser-trusted certificate authorities (CAs) owned and operated by Symantec improperly issued more than 100 unvalidated [transport layer security](#) certificates. In some cases, those certificates made it possible to spoof HTTPS-protected websites.

<http://arstechnica.com/security/2017/01/already-on-probation-symantec-issues-more-illegit-https-certificates/>

Misissued/Suspicious Symantec Certificates

Andrew Ayer | Thu, 19 Jan 2017 13:47:06 -0800

I. Misissued certificates for example.com

On 2016-07-14, Symantec misissued the following certificates for example.com:

<https://crt.sh/?sha256=A8F14F52CC1282D7153A13316E7DA39E6AE37B1A10C16288B9024A9B9DC3C4C6>

<https://crt.sh/?sha256=8B5956C57FDCF720B6907A4B1BC8CA2E46CD90EAD5C061A426CF48A6117BF8FA>

<https://crt.sh/?sha256=94482136A1400BC3A1136FECA3E79D4D200E03DD20B245D19F0E78B5679EAF48>

<https://crt.sh/?sha256=C69AB04C1B20E6FC7861C67476CADD1DAE7A8DCF6E23E15311C2D2794BFCDD1>

I confirmed with ICANN, the owner of example.com, that they did not authorize these certificates. These certificates were already revoked at the time I found them.

II. Suspicious certificates for domains containing the word "test"

On 2016-11-15 and 2016-10-26, Symantec issued certificates for various domains containing the word "test" which I strongly suspect were misissued:

With unpleasant consequences
when it all goes wrong

With unpleasant consequences when it all goes wrong

... in the leadership.
... sters helped ignited
... ountry's 45-member

... television interview.
Société Générale, BNP Paribas and
Crédit Agricole, are considered integral
actors in the French economy, lending

VOLATILITY IS THE NEW MARKET NORM
Large swings in share prices are more
common now than at any other time in
recent stock market history. PAGE 16

talk
ow

Iranian activists feel the chill as hacker taps into e-mails

BY SOMINI SENGUPTA

Cuba aimed at U.S.
her husband not to
anything happens,
stay right here with
told him in October
to be with you, and I
ou, and the children
without you."

He claims to be 21 years old, a student of
software engineering in Tehran who
reveres Ayatollah Ali Khamenei and
despises dissidents in his country.
He sneaked into the computer sys-
tems of a security firm on the outskirts
of Amsterdam. He created fake creden-
tials that could allow someone to spy on
Internet connections that appeared to
be secure. He then shared that bounty
with people he declines to identify.
The fruits of his labor are believed to
include tapping into the online
e-mails of many as 300,000
people last summer.

online security mechanism that is trusted
by Internet users all over the world.
Comodohacker, as he calls himself, in-
sists that he acted on his own and is un-
perturbed by the notion that his work
might have been used to spy on anti-
government compatriots.

"I'm totally independent," he said in
an e-mail exchange with The New York
Times. "I just share my findings with
some people in Iran. They are free to do
anything they want with my findings
and things I share with them, but I'm
not responsible."

In the
is most
recker,
HACKER, THE

What's going wrong here?

- The TLS handshake cannot specify WHICH CA should be used to validate the digital certificate
- Your browser will allow ANY CA to be used to validate a certificate

What's going wrong here?

- The TLS handshake cannot specify WHICH CA should be used to validate a digital certificate
WOW! That's awesomely bad!
- Your browser will allow ANY CA to be used to validate a certificate

What's going wrong here?

- The TLS handshake cannot specify WHICH CA should be used to *WOW! That's awesomely bad!* digital

- You
val



Here's a lock - it might be the lock on your front door for all i to know.

The lock might LOOK secure, but don't worry - literally ANY key can open it!

What's going wrong here?

- There is no incentive for quality in the CA marketplace
- Why pay more for any certificate when the entire CA structure is only as strong as the weakest CA
- And you browser trusts a LOT of CAs!
 - About 60 – 100 CA's
 - About 1,500 Subordinate RA's
 - Operated by 650 different organisations

See the EFF SSL observatory

<http://www.eff.org/files/DefcomSSLiverse.pdf>

In a commercial environment

Where CA's compete with each other for market share

And quality offers no protection

Than what 'wins' in the market?

Sustainable
Resilient

Secure

Privacy

Trusted

?

In a commercial environment

Where CA's compete with each other for market share

And quality offers no protection

Than what 'wins' in the market?

Sustainable
Resilient

Secure

Privacy

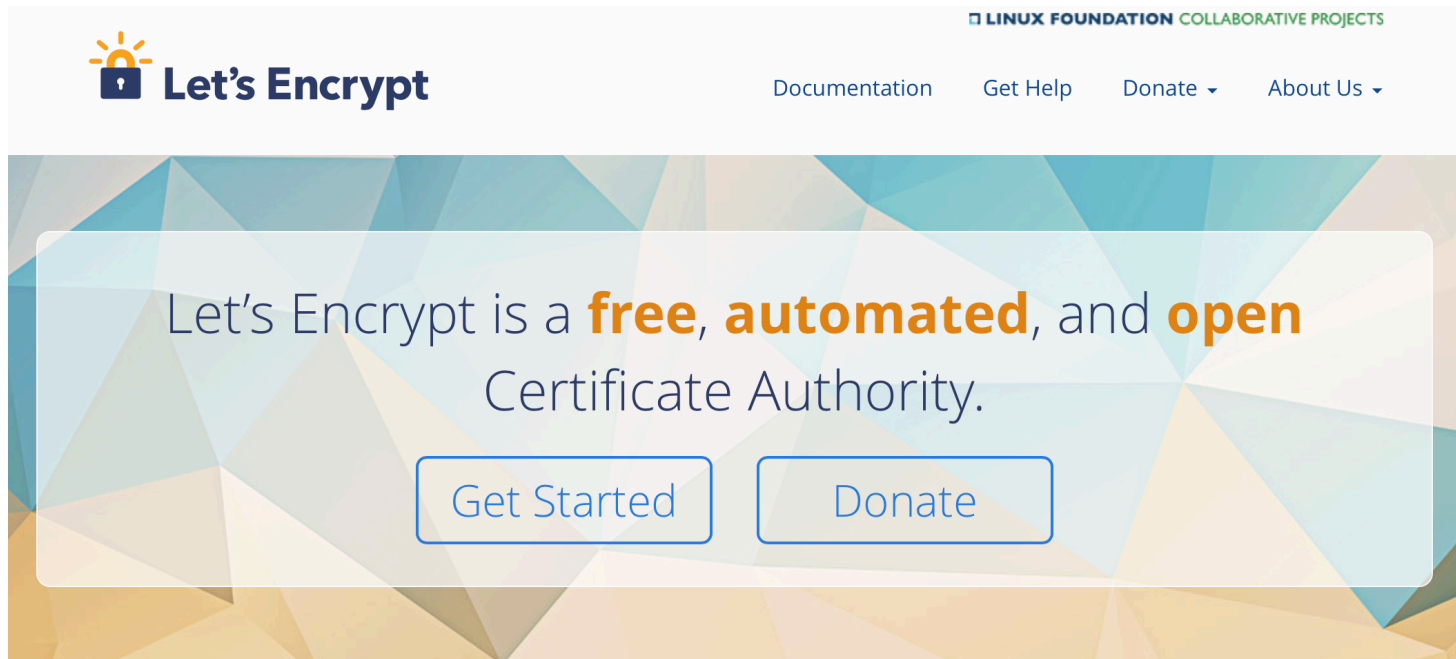
Trusted



Cheap!

Where now?

Option A: Take all the money out of the system!



The image shows a screenshot of the Let's Encrypt website. At the top left is the Let's Encrypt logo, which consists of a blue padlock with a yellow sunburst above it, followed by the text "Let's Encrypt" in a dark blue font. To the right of the logo, in the top right corner, is the text "LINUX FOUNDATION COLLABORATIVE PROJECTS" in a small, green, sans-serif font. Below this, there are four navigation links: "Documentation", "Get Help", "Donate" (with a small downward arrow), and "About Us" (with a small downward arrow). The main content area features a large, semi-transparent white box with a blue and orange geometric pattern in the background. Inside this box, the text reads: "Let's Encrypt is a **free, automated, and open** Certificate Authority." Below this text are two buttons: "Get Started" and "Donate", both with blue borders and blue text.

Let's Encrypt

LINUX FOUNDATION COLLABORATIVE PROJECTS

Documentation Get Help Donate ▾ About Us ▾

Let's Encrypt is a **free, automated, and open** Certificate Authority.

Get Started Donate

Where now?

Option A: Take all the money out of the system!

The image shows a screenshot of the Let's Encrypt website. At the top left is the Let's Encrypt logo, which consists of a sun icon above a padlock icon, followed by the text "Let's Encrypt". To the right of the logo is the text "LINUX FOUNDATION COLLABORATIVE PROJECTS". Below this are navigation links: "Documentation", "Get Help", "Donate", and "About Us". The main content area has a blue and orange geometric background. Overlaid on this is a white rectangular box containing handwritten text in brown ink. The text reads: "Will the automation of the Cert issuance coupled with a totally free service make the overall environment more or less secure?". Below this text are two buttons: "Get Started" and "Donate". At the bottom of the white box, another line of handwritten text says: "We're probably going to find out real soon!".

Let's Encrypt is a free, automated, and open Certificate Authority.

Get Started Donate

We're probably going to find out real soon!

Where now?

Option B: White Listing and Pinning with HSTS

https://code.google.com/p/chromium/codesearch#chromium/src/net/http/transport_security_state_static.json

```
transport_security_state_static.json  Layers Find
1 // Copyright (c) 2012 The Chromium Authors. All rights reserved.
2 // Use of this source code is governed by a BSD-style license that can be
3 // found in the LICENSE file.
4
5 // This file contains the HSTS preloaded list in a machine readable format.
6
7 // The top-level element is a dictionary with two keys: "pinsets" maps details
8 // of certificate pinning to a name and "entries" contains the HSTS details for
9 // each host.
10 //
11 // "pinsets" is a list of objects. Each object has the following members:
12 //   name: (string) the name of the pinset
13 //   static_spki_hashes: (list of strings) the set of allowed SPKIs hashes
14 //   bad_static_spki_hashes: (optional list of strings) the set of forbidden
15 //     SPKIs hashes
16 //   report_uri: (optional string) the URI to send violation reports to;
17 //     reports will be in the format defined in RFC 7469
18 //
19 // For a given pinset, a certificate is accepted if at least one of the
20 // "static_spki_hashes" SPKIs is found in the chain and none of the
21 // "bad_static_spki_hashes" SPKIs are. SPKIs are specified as names, which must
22 // match up with the file of certificates.
23 //
```

Where now?

Option B: White Listing and Pinning with HSTS

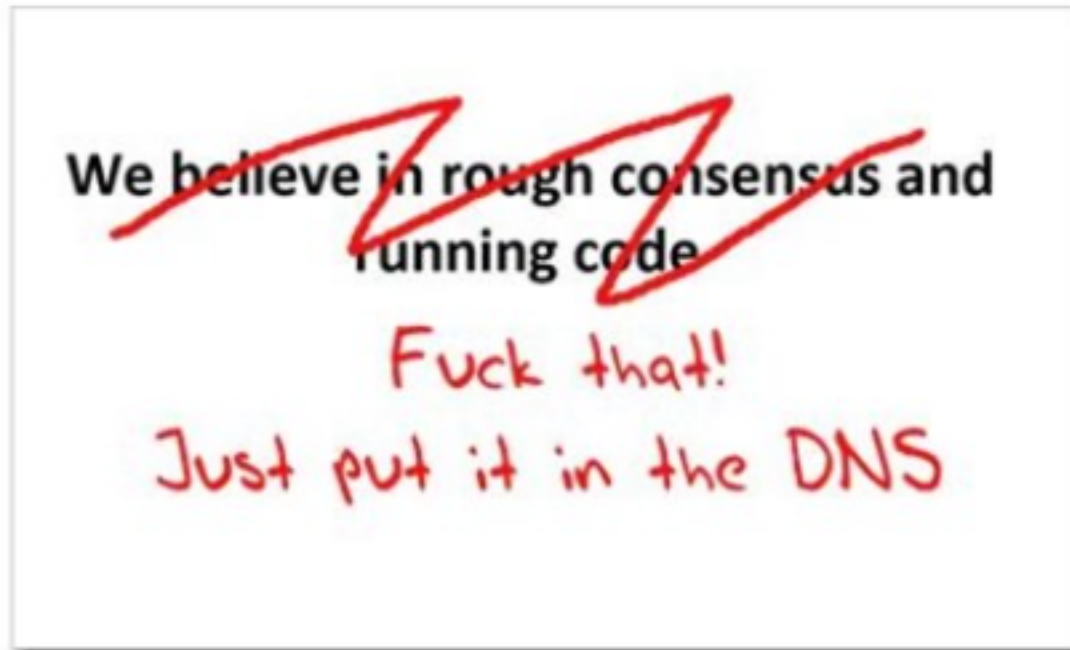
https://code.google.com/p/chromium/codesearch#chromium/transport_security/state_static

its not a totally insane idea -- until you realise that it appears to be completely unscalable!

```
1 // Copyright (c) 2012 The Chromium Authors. All rights reserved.
2 // Use of this source code is governed by a BSD-style license that can be
3 // found in the LICENSE file.
4
5 // This file contains the HSTS preloaded list in a machine readable format.
6
7 // The top-level element is a dictionary with two keys: "pinsets" maps details
8 // of certificate pinning to a name and "entries" contains the HSTS details for
9 // each host.
10 //
11 // "pinsets" is a list of objects. Each object has the following members:
12 //   name: (string) the name of the pinset
13 //   static_spki_hashes: (list of strings) the set of allowed SPKIs hashes
14 //   bad_static_spki_hashes: (optional list of strings) the set of forbidden
15 //     SPKIs hashes
16 //   report_uri: (optional string) the URI to send violation reports to;
17 //     reports will be in the format defined in RFC 7469
18 //
19 // For a given pinset, a certificate is accepted if at least one of the
20 // "static_spki_hashes" SPKIs is found in the chain and none of the
21 // "bad_static_spki_hashes" SPKIs are. SPKIs are specified as names, which must
22 // match up with the file of certificates.
23 //
```

Where now?

Option C: Use the DNS!



Seriously

Where better to find out the public key associated with a DNS-named service than to look it up in the DNS?

Seriously

Where better to find out the public key associated with a DNS-named service than to look it up in the DNS?

- Why not query the DNS for the HSTS record (pinning record)?

Seriously

Where better to find out the public key associated with a DNS-named service than to look it up in the DNS?

- Why not query the DNS for the HSTS record?
- Why not query the DNS for the issuer CA?

Seriously

Where better to find out the public key associated with a DNS-named service than to look it up in the DNS?

- Why not query the DNS for the HSTS record?
- Why not query the DNS for the issuer CA?
- Why not query the DNS for the hash of the domain name cert?

Seriously

Where better to find out the public key associated with a DNS-named service than to look it up in the DNS?

- Why not query the DNS for the HSTS record?
- Why not query the DNS for the issuer CA?
- Why not query the DNS for the hash of the domain name cert?
- Why not query the DNS for the hash of the domain name public key?

Seriously

Where better to find out the public key associated with a DNS-named service than to look it up in the DNS?

- Why not query the HSTS record?
- Why not query the DNS for the issuer CA?
- Why not query the DNS for the hash of the domain name cert?

- Why not query the DNS for the hash of the domain name public key?

Who needs CA's anyway?

Seriously

Where better to find out the public key associated with a DNS-named service than to look it up in the DNS?

- Why not query the DNS for the HSTS record?
- Why not query the DNS for the issuer CA?
- Why not query the DNS for the main name cert?

Who needs CA's anyway?

Secure your fans with an SSL Certificate.

Keep your customers' private data out of the wrong hands.

As low as
\$74.99/yr

Get your business online with a team domain.

Now just
\$10.99/yr

Find Your .com.au

Why not query the DNS for the hash of the main name public key?

DANE

- Using the DNS to associated domain name public key certificates with domain name

[\[Docs\]](#) [\[txt|pdf\]](#) [\[draft-ietf-dane-p...\]](#) [\[Diff1\]](#) [\[Diff2\]](#) [\[Errata\]](#)

Updated by: [7218](#), [7671](#) PROPOSED STANDARD

Internet Engineering Task Force (IETF) Errata Exist

Request for Comments: 6698 P. Hoffman

Category: Standards Track VPN Consortium

ISSN: 2070-1721 J. Schlyter

Kirei AB

August 2008

The DNS-Based Authentication of Names
Transport Layer Security

Abstract

Encrypted communication on the Internet often uses Transport Layer Security (TLS). This depends on third parties to certify the keys used. This document improves on that situation by enabling the administrators of domain names to specify the keys used in that domain's TLS servers. This requires matching improvements in TLS client software, but no change in TLS server software.

Status of This Memo

This is an Internet Standards Track document.

RFC 6698 -- You should read this!

DANE

- Using the DNS to associated domain name public key certificates with domain name

[Docs] [txt|pdf] [draft-ietf-dane-ops] [Diff1] [Diff2]

PROPOSED STANDARD

Internet Engineering Task Force (IETF) V. Dukhovni
Request for Comments: 7671 Two Sigma
Updates: 6698 W. Hardaker
Category: Standards Track
ISSN: 2070-1721

The DNS-Based Authentication of Names (DANE) TLSA specification (RFC 6698), based on Updates and Protocol:

Abstract

Updates and updates the DNS-Based Authentication of Names (DANE) TLSA specification (RFC 6698), based on subsequent implementation experience. It also contains guidance for implementers, operators, and protocol developers who want to use DANE records.

Status of This Memo

This is an Internet Standards Track document.

You probably should read RFC 7671 as well!

DANE

TLSA RR

2.3. TLSA RR Examples

An example of a hashed (SHA-256) association of a PKIX CA certificate:

```
_443._tcp.www.example.com. IN TLSA (  
  0 0 1 d2abde240d7cd3ee6b4b28c54df034b9  
      7983ald16e8a410e4561cb106618e971 )
```

CA Cert Hash

An example of a hashed (SHA-512) subject public key association of a PKIX end entity certificate:

```
_443._tcp.www.example.com. IN TLSA  
  1 1 2 92003ba34942dc74152e2f2c408d29ec  
      a5a520e7f2e06bb944f4dca346baf63c  
      1b177615d466f6c4b71c216a50292bd5  
      8c9ebdd2f74e38fe51ffd48c43326cbc )
```

EE Cert Hash

An example of a full certificate association of a PKIX trust anchor:

```
_443._tcp.www.example.com. IN TLSA  
  2 0 0 30820307308201efa003020102020... )
```

Trust Anchor

EECCert TLSA record generation

```
; Convert the public key certificate to DER format  
; Generate the SHA256 hash  
; Add DNS gunk!
```

```
$ /usr/bin/openssl x509 -in /usr/local/etc/letsencrypt/live/www.dotnxdomain.net/cert.pem -outform DER |  
/usr/bin/openssl sha256 |  
cut -d ' ' -f 2 |  
awk '{print "_443._tcp.www.dotnxdomain.net  IN TLSA 3 0 1 " $1}'
```

```
_443._tcp.www.dotnxdomain.net. 899 IN      TLSA 3 0 1 D42101BCCE941D22E8E467C5D75E77EC4A7B8B7C9366C6A878CB4E15 7E602F17
```

```
$ dig +dnssec TLSA _443._tcp.www.dotnxdomain.net.
```

```
_443._tcp.www.dotnxdomain.net. 899 IN      TLSA 3 0 1 D42101BCCE941D22E8E467C5D75E77EC4A7B8B7C9366C6A878CB4E15 7E602F17  
_443._tcp.www.dotnxdomain.net. 899 IN      RRSIG TLSA 13 5 900 20200724235900 20170122043100 56797 www.dotnxdomain.net.  
dUYD1sMIpBc6RsUhturFzz5G8qX6oaDGRzaD/q6n+YJi2kqzDfWZls6F 3X1mXdpeQQYz52y0U0cdWvFR09TQZQ==
```

SPKI TLSA record generation

- ; Generate the public key
- ; Convert it to DER format
- ; Generate the SHA256 hash
- ; Add DNS gunk!

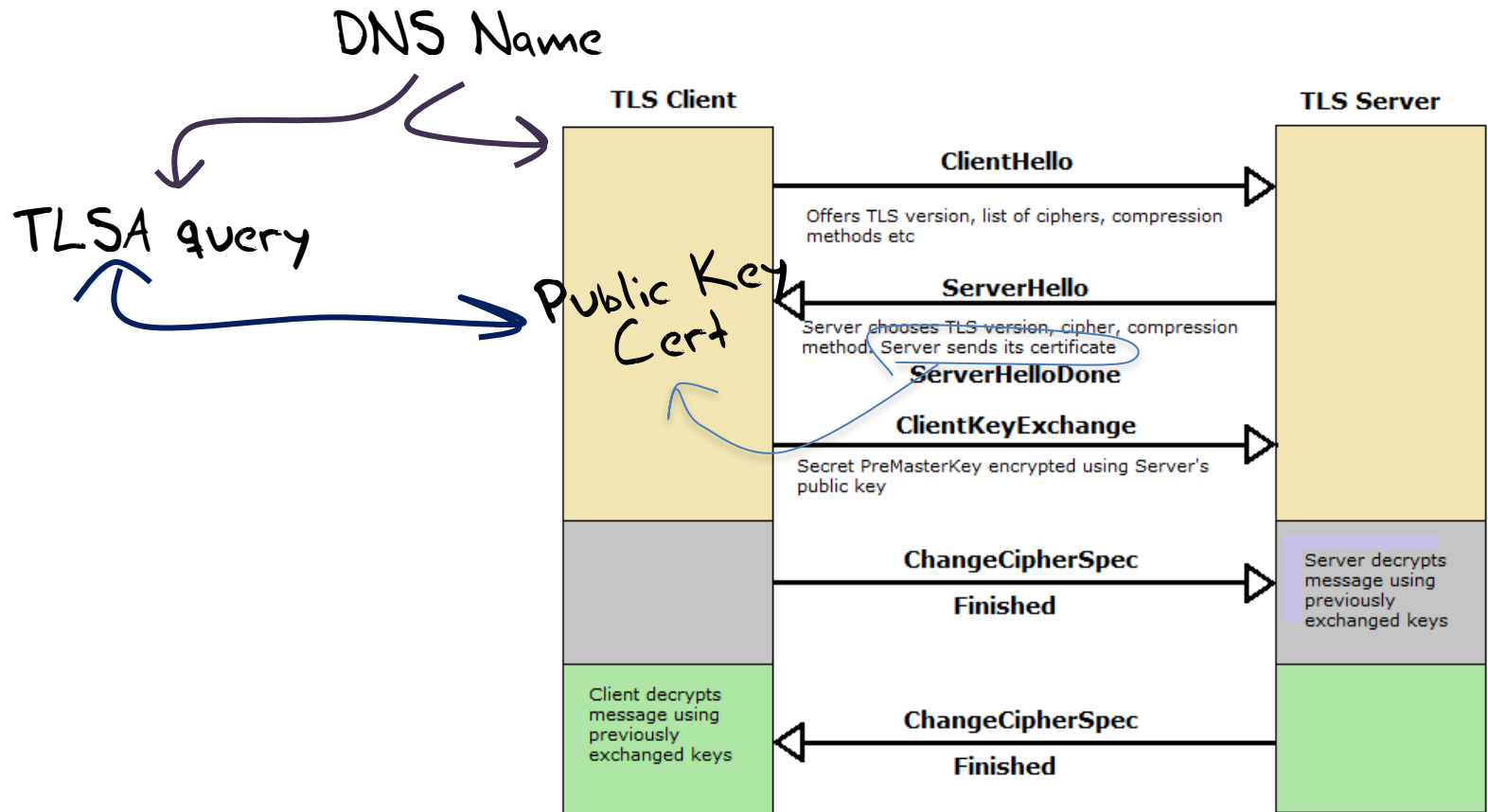
```
$ /usr/bin/openssl x509 -in /usr/local/etc/letsencrypt/live/www.dotnxdomain.net/cert.pem -pubkey -noout |  
openssl rsa -pubin -outform der |  
/usr/bin/openssl sha256 |  
cut -d ' ' -f 2 |  
awk '{ print "_443._tcp.www.ndotnxdomain.net IN TLSA 3 1 1 " $1}'
```

```
_443._tcp.www.ndotnxdomain.net IN TLSA 3 1 1 df3a810d998cfddf8fa935ed33065ee27a67747366e2da40ddefef2b3a2032eb
```

TLS with DANE

- Client receives server cert in Server Hello
 - *Client lookups the DNS for the TLSA Resource Record of the domain name*
 - *Client validates the presented certificate against the TLSA RR*
- Client performs Client Key exchange

TLS Connections



Just one problem...

- The DNS is full of liars and lies!
- And this can compromise the integrity of public key information embedded in the DNS
- Unless we fix the DNS we are no better off than before with these TLSA records!

Just one response...

- We need to allow users to validate DNS responses for themselves
- And for this we need a Secure DNS framework
- Which we have – and its called DNSSEC!

DNSSEC Interlocking Signatures

. (root)

- . Key-Signing Key – signs over
 - . Zone-Signing Key – signs over
 - DS for .com (Key-Signing Key)

.com

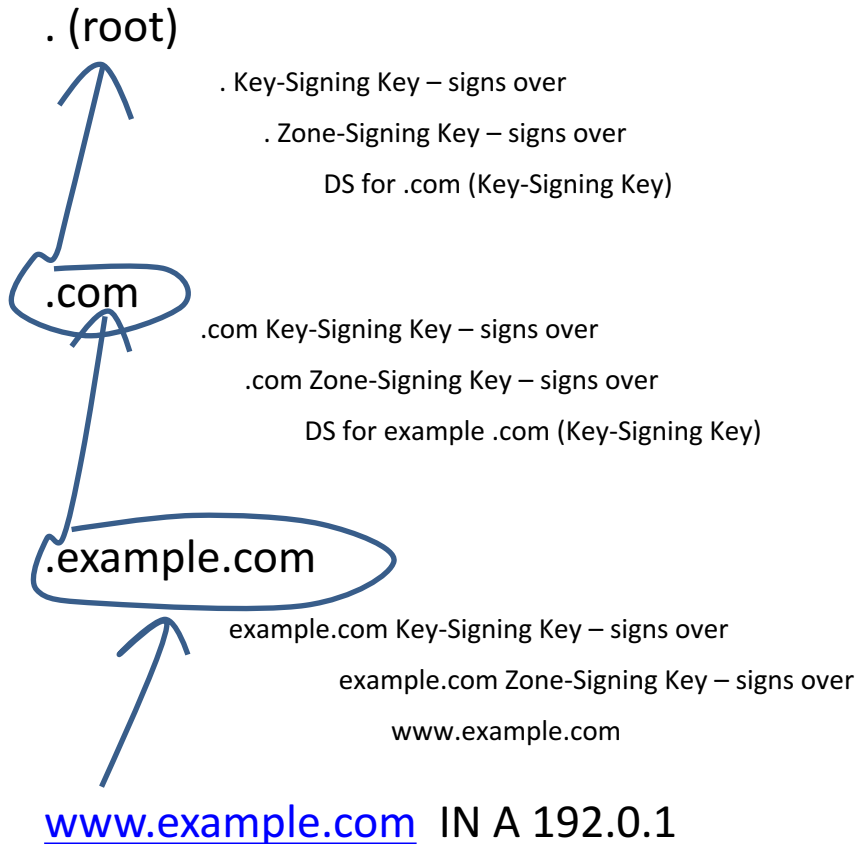
- .com Key-Signing Key – signs over
 - .com Zone-Signing Key – signs over
 - DS for example .com (Key-Signing Key)

.example.com

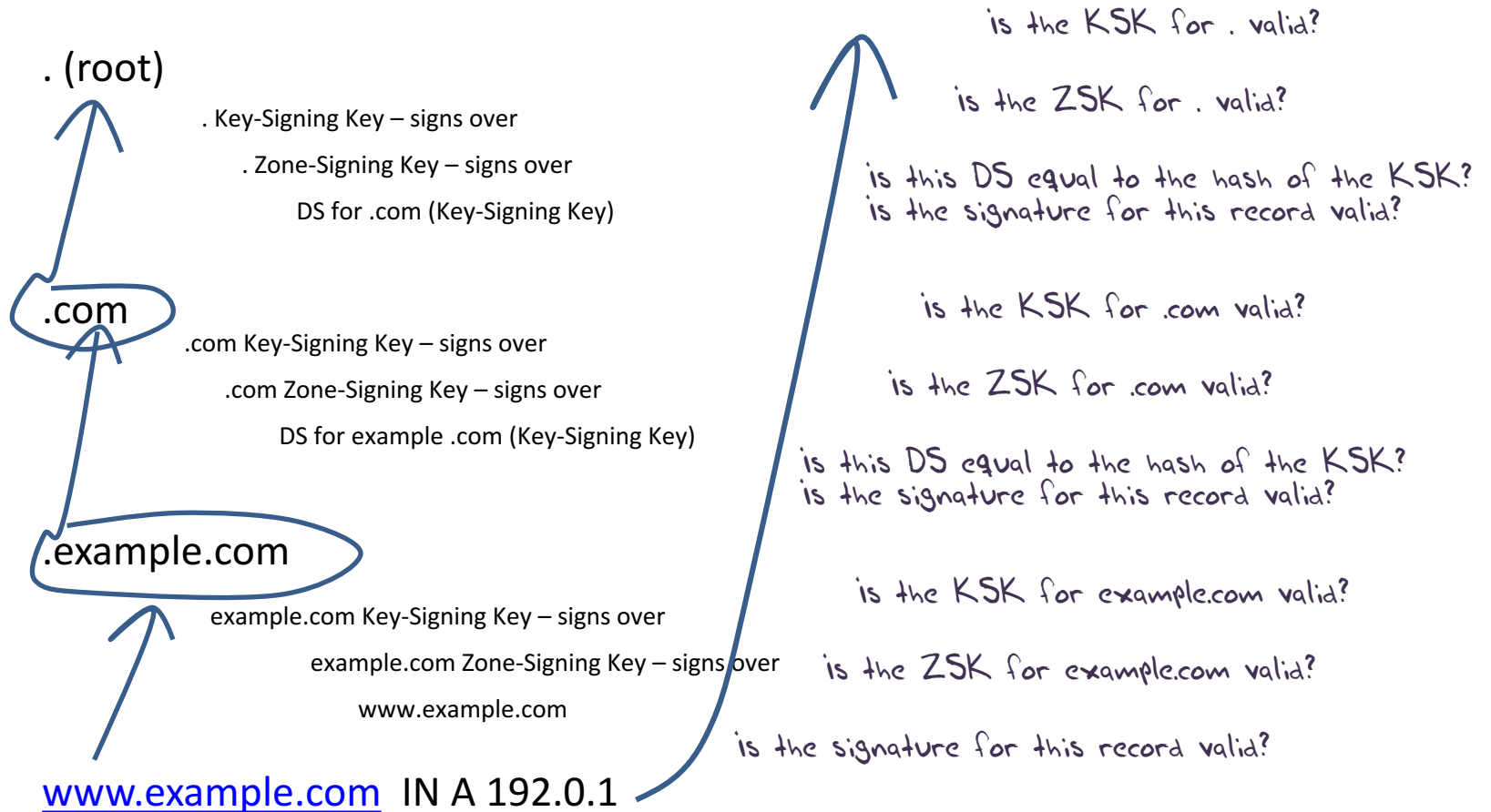
- example.com Key-Signing Key – signs over
 - example.com Zone-Signing Key – signs over
 - www.example.com

www.example.com

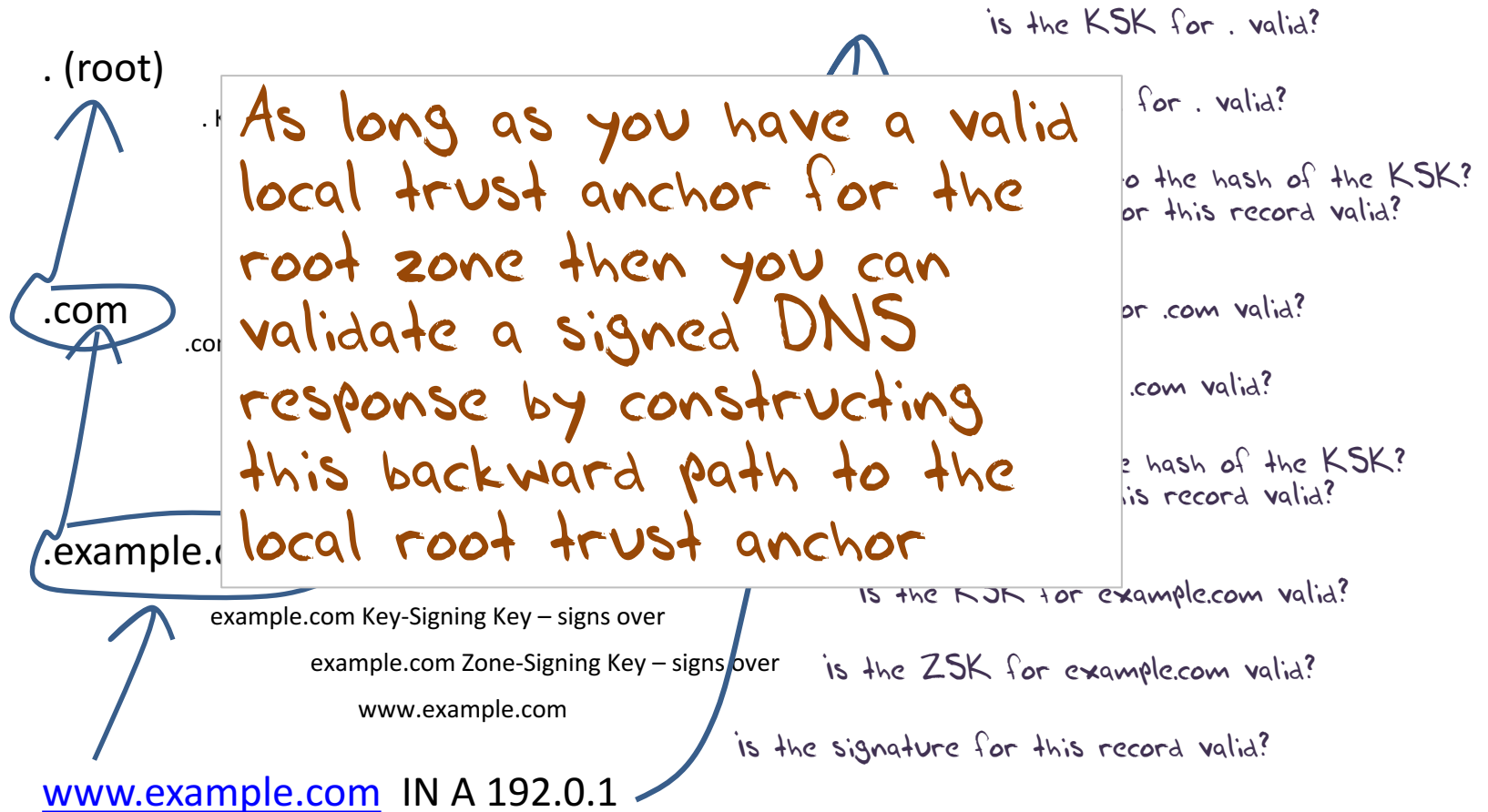
DNSSEC Interlocking Signatures



DNSSEC Interlocking Signatures



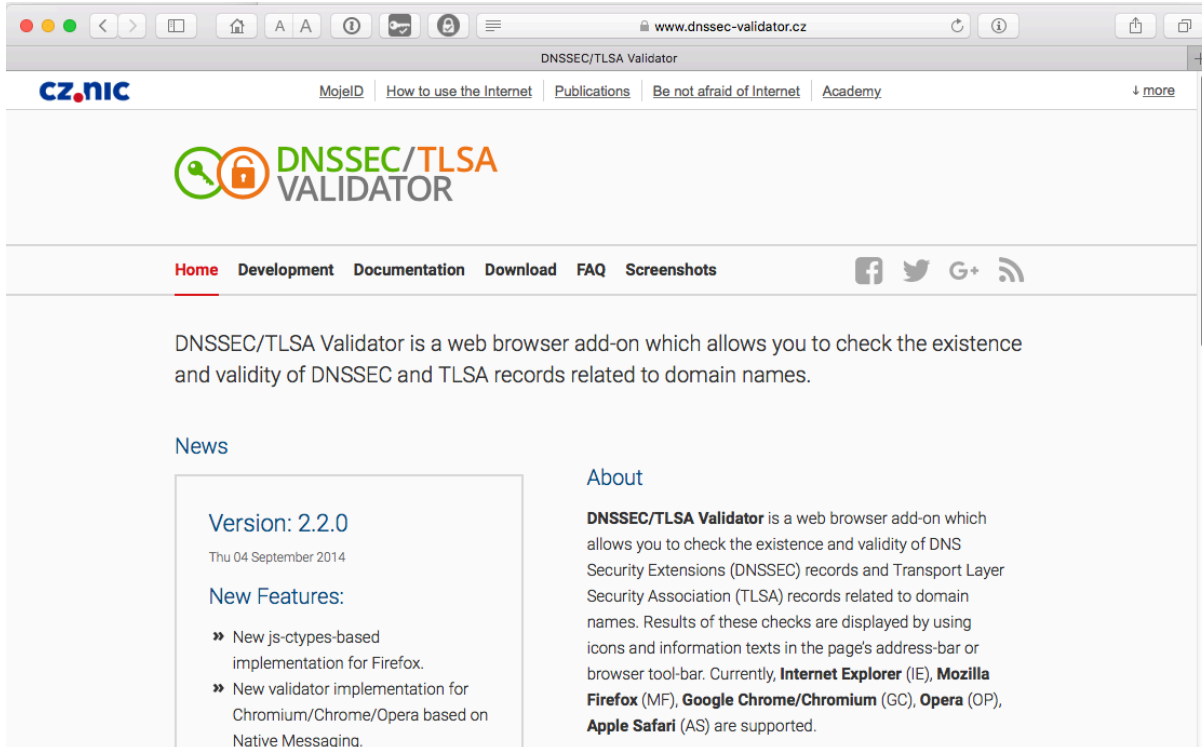
DNSSEC Interlocking Signatures



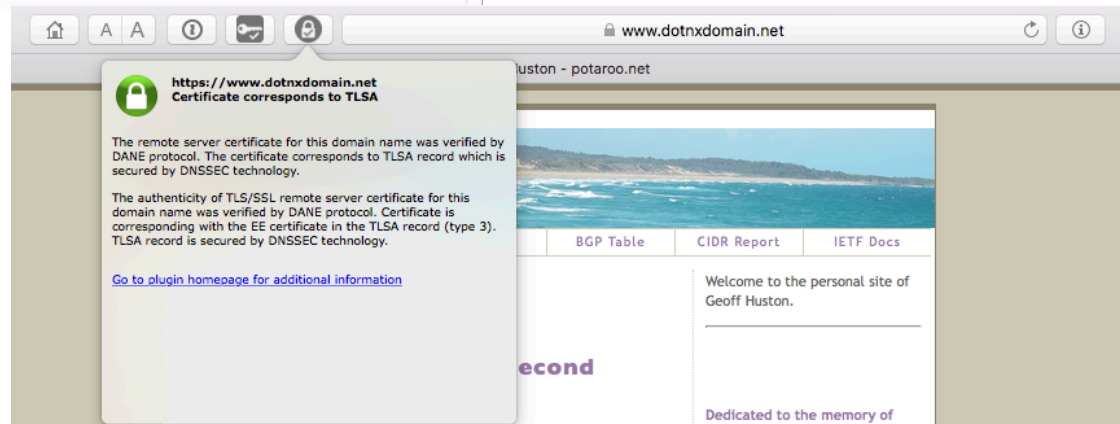
DANE + DNSSEC

- Query the DNS for the TLSA record of the domain name and ask for the DNSSEC signature to be included in the response
- Validate the signature to ensure that you have an unbroken signature chain to the root trust point
- At this point you can accept the TLSA record as the authentic record, and set up a TLS session based on this data

DANE Does DNS via a Browser Extension



The screenshot shows the website for the DNSSEC/TLSA Validator. The browser's address bar displays 'www.dnssec-validator.cz'. The website features a navigation menu with links for 'Home', 'Development', 'Documentation', 'Download', 'FAQ', and 'Screenshots'. A main heading reads 'DNSSEC/TLSA Validator is a web browser add-on which allows you to check the existence and validity of DNSSEC and TLSA records related to domain names.' Below this, there are sections for 'News' and 'About'. The 'News' section highlights 'Version: 2.2.0' dated 'Thu 04 September 2014' and lists 'New Features' such as 'New js-ctypes-based implementation for Firefox' and 'New validator implementation for Chromium/Chrome/Opera based on Native Messaging'. The 'About' section describes the add-on's purpose and lists supported browsers: Internet Explorer (IE), Mozilla Firefox (MF), Google Chrome/Chromium (GC), Opera (OP), and Apple Safari (AS).



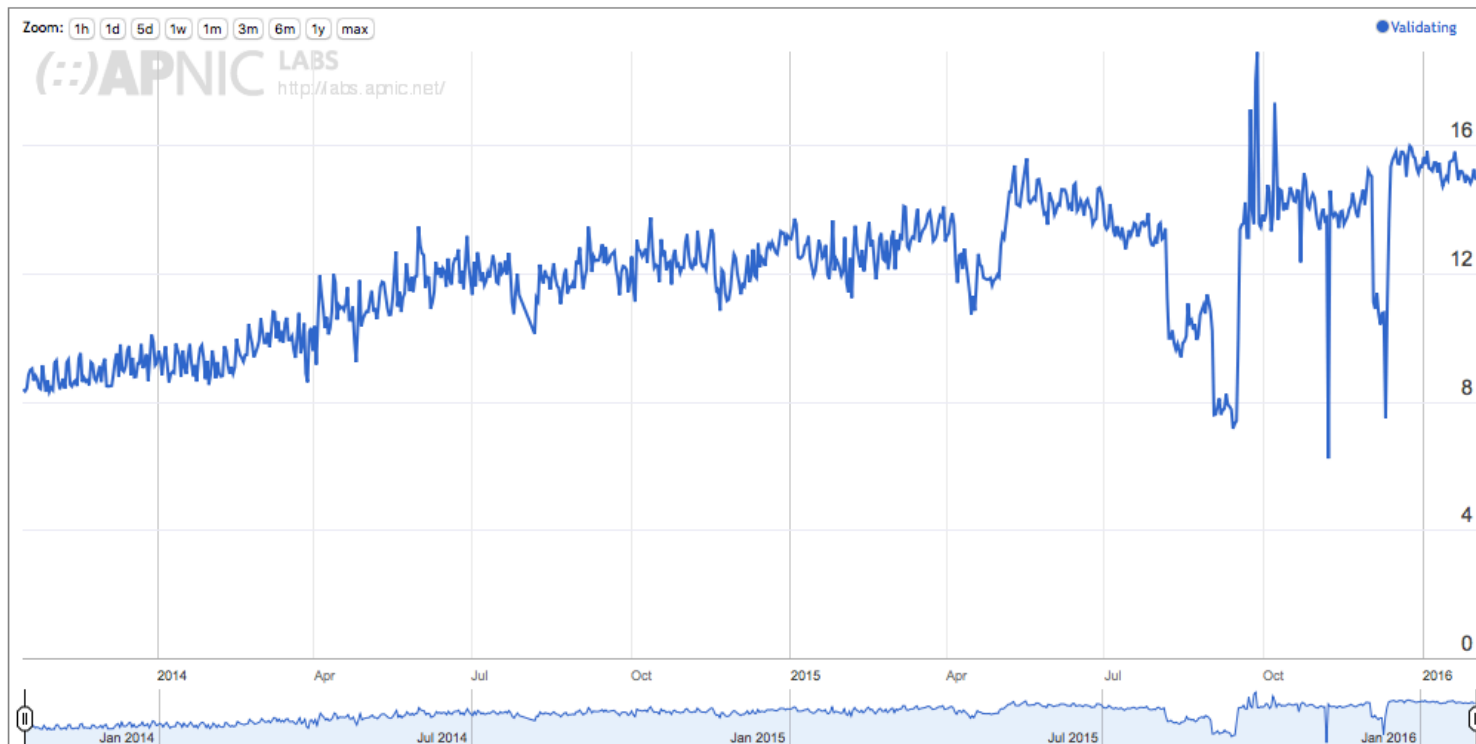
This screenshot shows a browser window with the address 'www.dotnxdomain.net'. A notification box is overlaid on the page, displaying a green padlock icon and the text: 'https://www.dotnxdomain.net Certificate corresponds to TLSA'. Below the notification, there is a detailed message: 'The remote server certificate for this domain name was verified by DANE protocol. The certificate corresponds to TLSA record which is secured by DNSSEC technology. The authenticity of TLS/SSL remote server certificate for this domain name was verified by DANE protocol. Certificate is corresponding with the EE certificate in the TLSA record (type 3). TLSA record is secured by DNSSEC technology.' A link is provided: 'Go to plugin homepage for additional information'. The background page shows a header with 'BGP Table', 'CIDR Report', and 'IETF Docs', and a welcome message: 'Welcome to the personal site of Geoff Huston.'

So we need DNSSEC as well
as DANE...

How much DNSSEC Validation is out there?

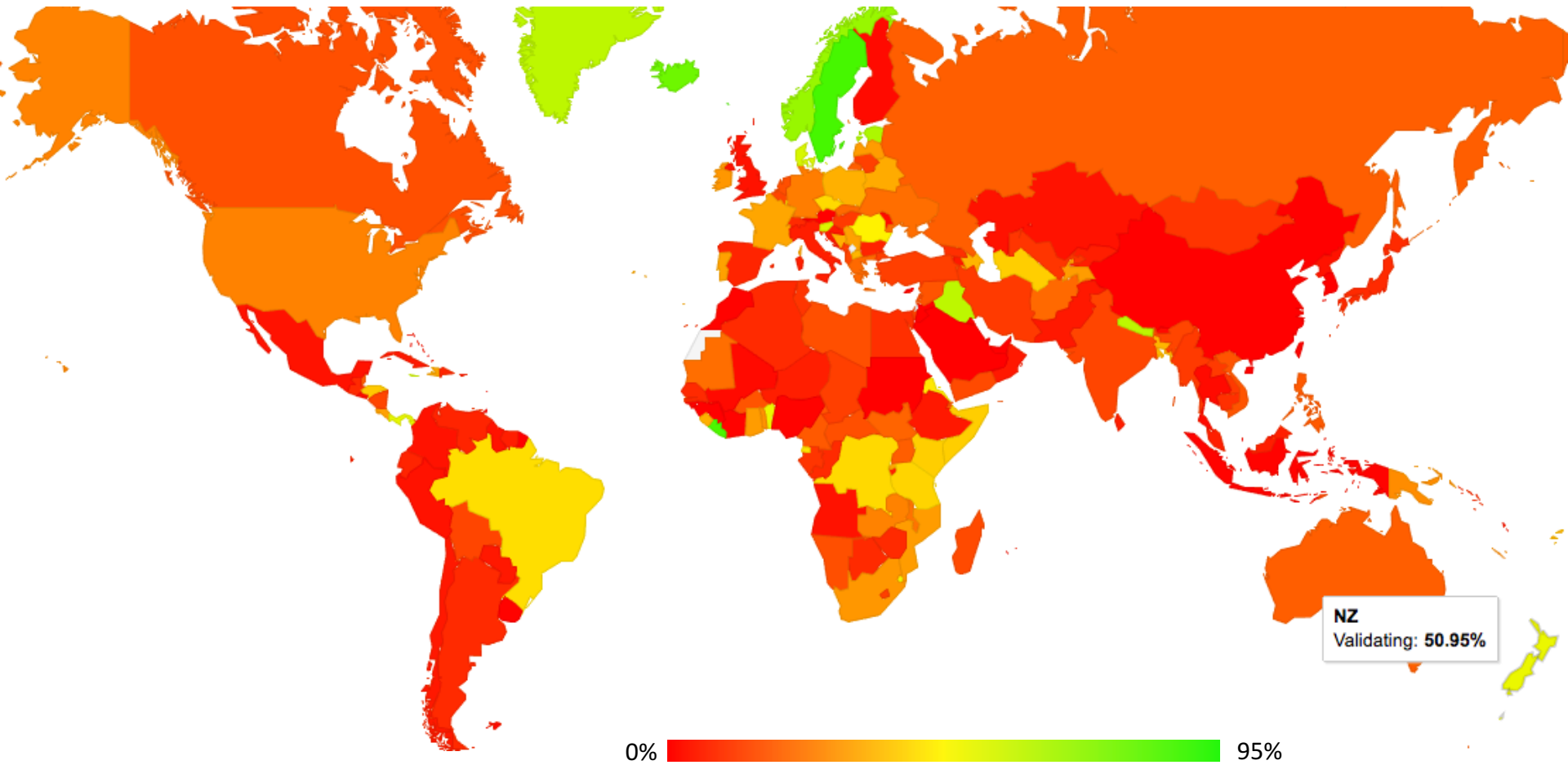
Do we do DNSSEC Validation?

Use of DNSSEC Validation for World (XA)



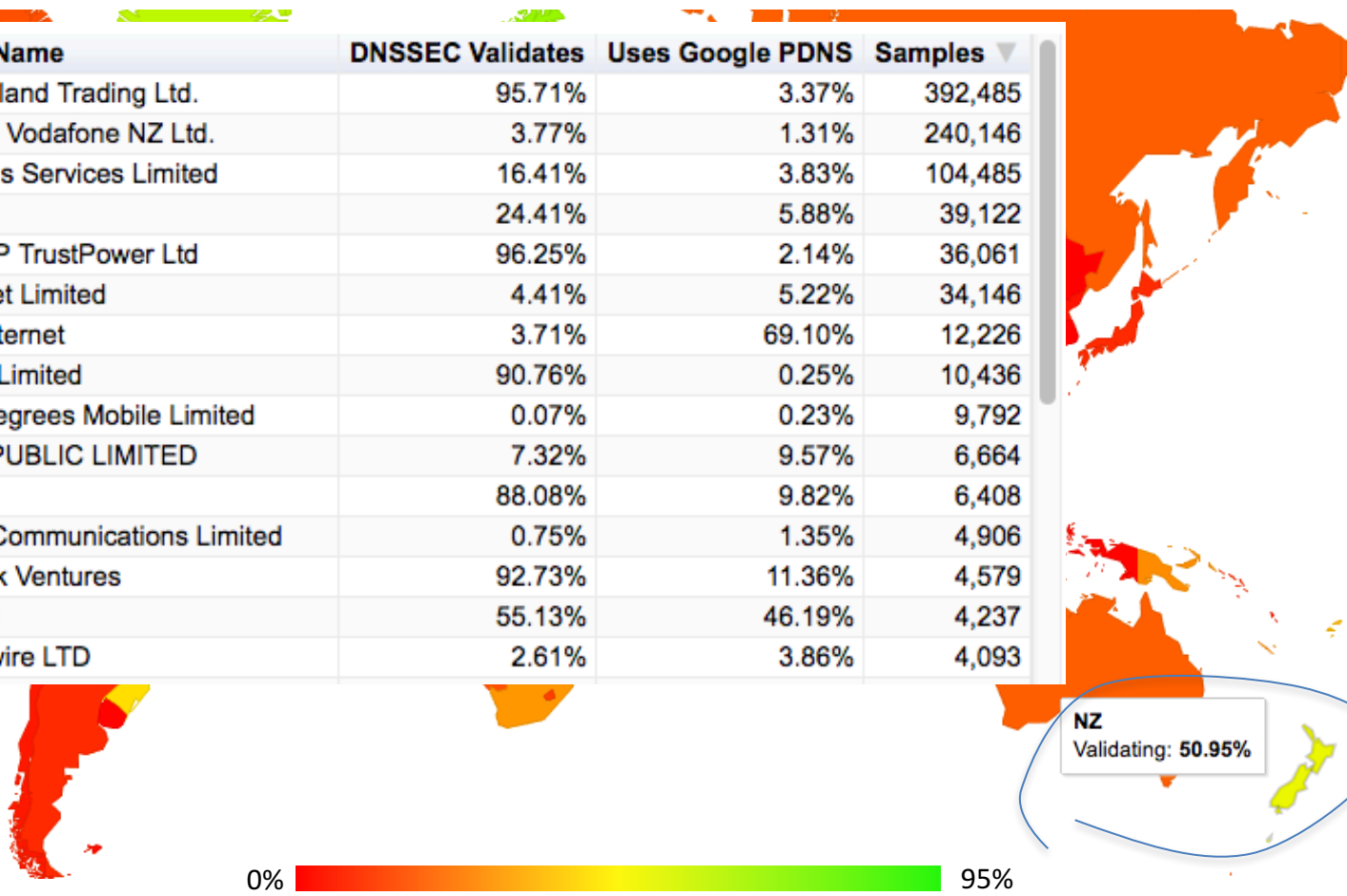
stats.labs.apnic.net/dnssec/XA

Do we do DNSSEC Validation?

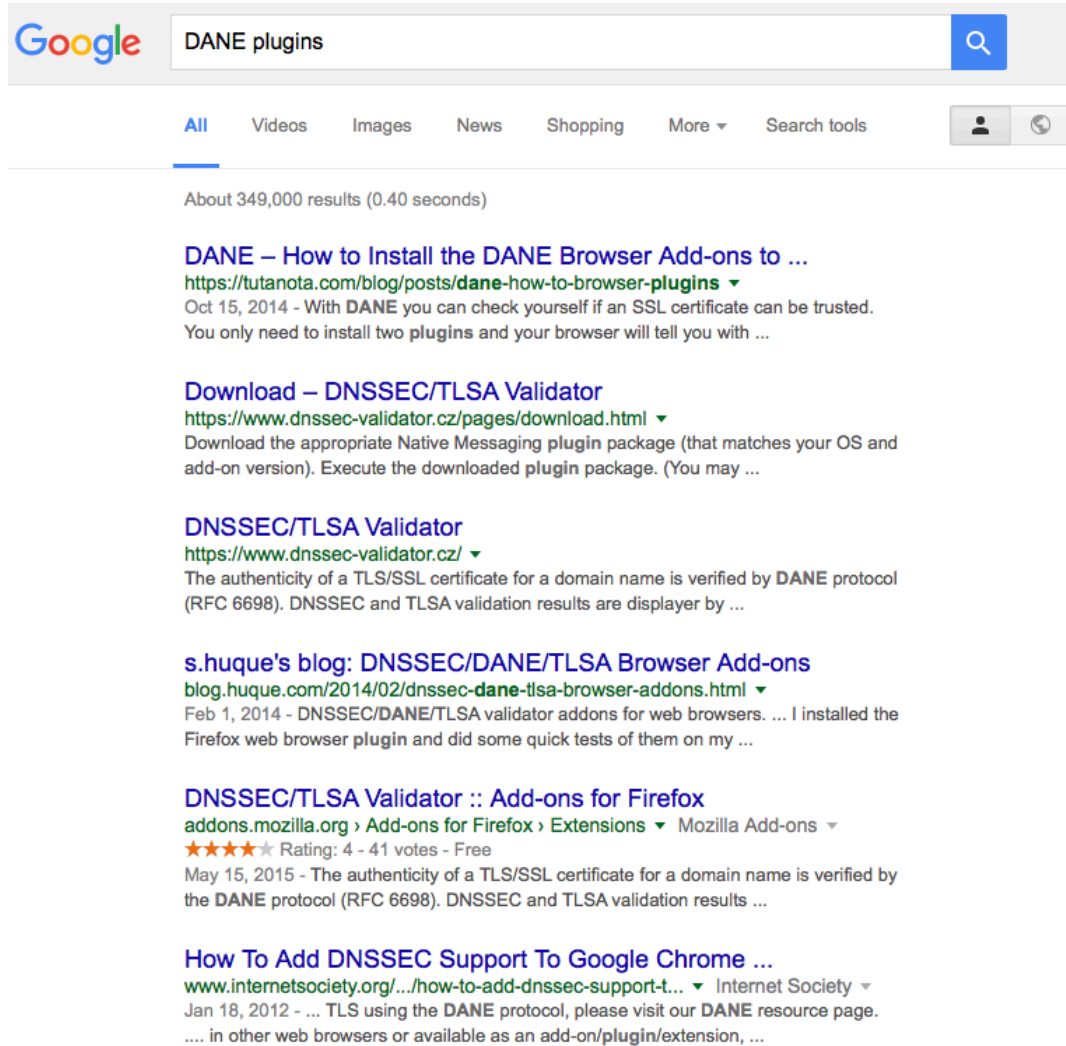


Do we do DNSSEC Validation?

ASN	AS Name	DNSSEC Validates	Uses Google PDNS	Samples
AS4771	SPARKNZ Spark New Zealand Trading Ltd.	95.71%	3.37%	392,485
AS9500	VODAFONE-TRANSIT-AS Vodafone NZ Ltd.	3.77%	1.31%	240,146
AS9790	CALLPLUS-NZ-AP CallPlus Services Limited	16.41%	3.83%	104,485
AS4768	CLIX-NZ TelstraClear Ltd	24.41%	5.88%	39,122
AS55850	TRUSTPOWERLTD-AS-AP TrustPower Ltd	96.25%	2.14%	36,061
AS23655	SNAP-NZ-AS Snap Internet Limited	4.41%	5.22%	34,146
AS4648	NZIX-2 Global-Gateway Internet	3.71%	69.10%	12,226
AS58600	FLIP-AS-AP Flip Services Limited	90.76%	0.25%	10,436
AS38793	NZCOMMS-AS-AP Two Degrees Mobile Limited	0.07%	0.23%	9,792
AS133579	MYREPNZ-AS-AP MYREPUBLIC LIMITED	7.32%	9.57%	6,664
AS9876	AIRNET-HB-AS-AP NOW	88.08%	9.82%	6,408
AS55872	BAYCITY-AS-AP BayCity Communications Limited	0.75%	1.35%	4,906
AS133124	SPARKVENT-AS-AP Spark Ventures	92.73%	11.36%	4,579
AS55853	MEGATEL-AS-AP Megatel	55.13%	46.19%	4,237
AS45267	LIGHTWIRE-AS-AP Lightwire LTD	2.61%	3.86%	4,093



Where now?



Google search results for "DANE plugins". The search bar shows "DANE plugins" and the search button is a magnifying glass icon. Below the search bar are navigation tabs: All, Videos, Images, News, Shopping, More, and Search tools. The search results show about 349,000 results in 0.40 seconds. The first result is "DANE – How to Install the DANE Browser Add-ons to ..." from tutanota.com, dated Oct 15, 2014. The second result is "Download – DNSSEC/TLSA Validator" from dnssec-validator.cz, dated Feb 1, 2014. The third result is "DNSSEC/TLSA Validator" from dnssec-validator.cz, dated Feb 1, 2014. The fourth result is "s.huque's blog: DNSSEC/DANE/TLSA Browser Add-ons" from blog.huque.com, dated Feb 1, 2014. The fifth result is "DNSSEC/TLSA Validator :: Add-ons for Firefox" from addons.mozilla.org, dated May 15, 2015. The sixth result is "How To Add DNSSEC Support To Google Chrome ..." from www.internetsociety.org, dated Jan 18, 2012.

Google

DANE plugins

All Videos Images News Shopping More Search tools

About 349,000 results (0.40 seconds)

DANE – How to Install the DANE Browser Add-ons to ...
<https://tutanota.com/blog/posts/dane-how-to-browser-plugins>
Oct 15, 2014 - With **DANE** you can check yourself if an SSL certificate can be trusted. You only need to install two **plugins** and your browser will tell you with ...

Download – DNSSEC/TLSA Validator
<https://www.dnssec-validator.cz/pages/download.html>
Download the appropriate Native Messaging **plugin** package (that matches your OS and add-on version). Execute the downloaded **plugin** package. (You may ...

DNSSEC/TLSA Validator
<https://www.dnssec-validator.cz/>
The authenticity of a TLS/SSL certificate for a domain name is verified by **DANE** protocol (RFC 6698). DNSSEC and TLSA validation results are displayed by ...

s.huque's blog: DNSSEC/DANE/TLSA Browser Add-ons
<blog.huque.com/2014/02/dnssec-dane-tlsa-browser-addons.html>
Feb 1, 2014 - DNSSEC/DANE/TLSA validator addons for web browsers. ... I installed the Firefox web browser **plugin** and did some quick tests of them on my ...

DNSSEC/TLSA Validator :: Add-ons for Firefox
<addons.mozilla.org> > Add-ons for Firefox > Extensions > Mozilla Add-ons >
★★★★★ Rating: 4 - 41 votes - Free
May 15, 2015 - The authenticity of a TLS/SSL certificate for a domain name is verified by the **DANE** protocol (RFC 6698). DNSSEC and TLSA validation results ...

How To Add DNSSEC Support To Google Chrome ...
<www.internetsociety.org/.../how-to-add-dnssec-support-t...>
Jan 18, 2012 - ... TLS using the **DANE** protocol, please visit our **DANE** resource page. ... in other web browsers or available as an add-on/**plugin**/extension, ...

Browser vendors appear to be dragging the chain on DANE support

DANE exists today as plug-ins rather than a core functionality

Cynically, one could observe that fast but insecure is the browser vendors' current preference!

Or...

Look - No DNS!

- Server packages server cert, TLSA record and the DNSSEC credential chain in a single bundle
- Client receives bundle in Server Hello
 - *Client performs validation of TLSA Resource Record using the supplied DNSEC signatures plus the local DNS Root Trust Anchor without performing any DNS queries*
 - *Client validates the presented certificate against the TLSA RR*
- Client performs Client Key exchange

Faster DANE with Stapling

Bug 672600 - Use DNSSEC/DANE chain stapled into TLS handshake in certificate chain [Last Comment](#)
validation

Status: REOPENED	Reported: 2011-07-19 12:05 PDT by David Keeler [:keeler] (use needinfo?)
Whiteboard: [psm-assigned]	Modified: 2016-11-18 01:39 PST (History)
Keywords:	CC List: 82 users (show)
Product: Core (show info)	See Also: 1201841
Component: Security: PSM (show other bugs) (show info)	Crash Signature: (edit)
Version: Trunk	QA Whiteboard:
Platform: All All	Iteration: ---
Importance: P1 enhancement with 81 votes (vote)	Points: ---
Target Milestone: ---	Has Regression Range: ---
Assigned To: Richard Barnes [:rbarnes]	Has STR: ---
QA Contact:	Tracking Flags:
Triage Owner: David Keeler [:keeler] (use needinfo?)	
Mentors:	
URL:	
Duplicates: 666148 1201841 (view as bug list)	
Depends on: 672596	
Blocks: 672239	
Show dependency tree / graph	

Mozilla Bug Report [672600](#)

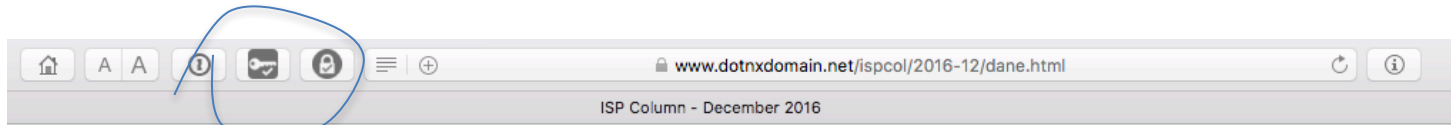
Where now?

We could do a **far** better job at Internet Security:

- Publishing DNSSEC-signed zones
- Publishing DANE TLSA records
- Using DNSSEC-validating resolution
- Using TLSA records to guide TLS Key Exchange



What this can offer is robust, affordable, accessible security without the current overheads of high priced vanity CA offerings

Let's Do it!



The ISP Column

A column on things Internet

Other Formats:  

Let's Encrypt with DANE

December 2016

Geoff Huston

There is a frequently quoted adage in communications that goes along the lines of "Good, Fast, Cheap: pick any two!" It may well be applied to many other forms of service design and delivery, but the basic idea is that high quality, high speed services are costly to obtain, and if you want a cheaper service that you need to compromise either on the speed of the service or its quality. However, if you looked at the realm of security, and X.509 certificate-based secure systems, we appear to be in the worst of all worlds: It can be expensive, inherently comprisable and slow to set up and access. So somehow we've managed to achieve: "Security: Poor, Slow and Expensive!"

However, this environment is changing, and it may no longer be the case. In this column I'd like to walk through the process of setting up good, inexpensive and accessible security using several public tools.

What I'll do here is a step by step log of my efforts to set up a secure web service using Let's Encrypt Domain Name public key X.509 certificates and DNSA TLSA records. I'm using a platform of a FreeBSD system running an Apache web server in this example. While the precise commands and configuration may be different for other OS platforms and other web servers, the underlying steps are much the same, and these steps can be readily ported.

What Let's Encrypt and DNSSEC offers is robust, affordable, accessible security without the current overheads of high priced vanity CA offerings

That's it!

Questions?