Why Dane?

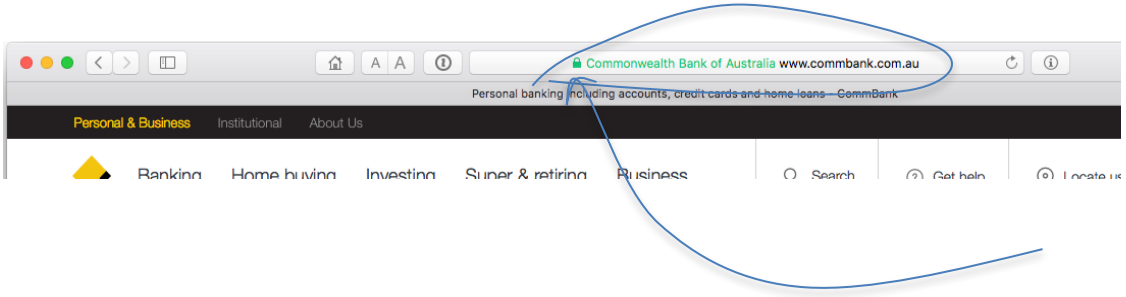
Geoff Huston
Chief Scientist, APNIC

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?



My Bank's web site

Or at least I think its my bank because it looks a bit familiar and there is a green icon of a lock

So it HAS to be my bank – hasn't it?

Connection 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.
```

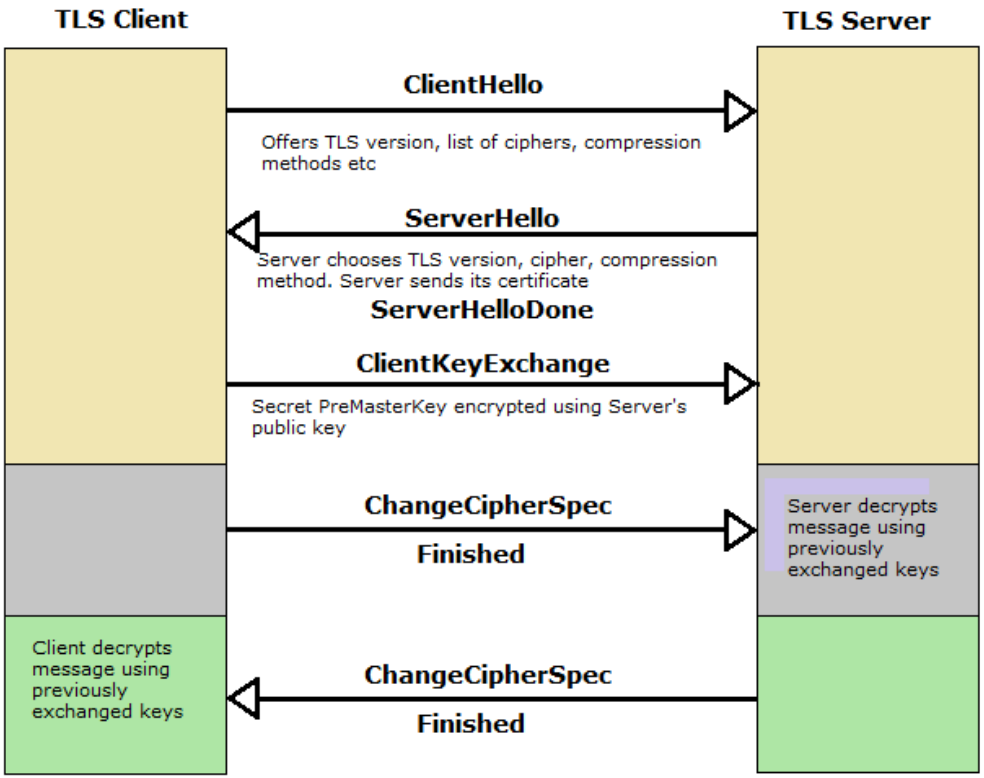
That's not an IP addresses that was allocated to the Commonwealth Bank!

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?

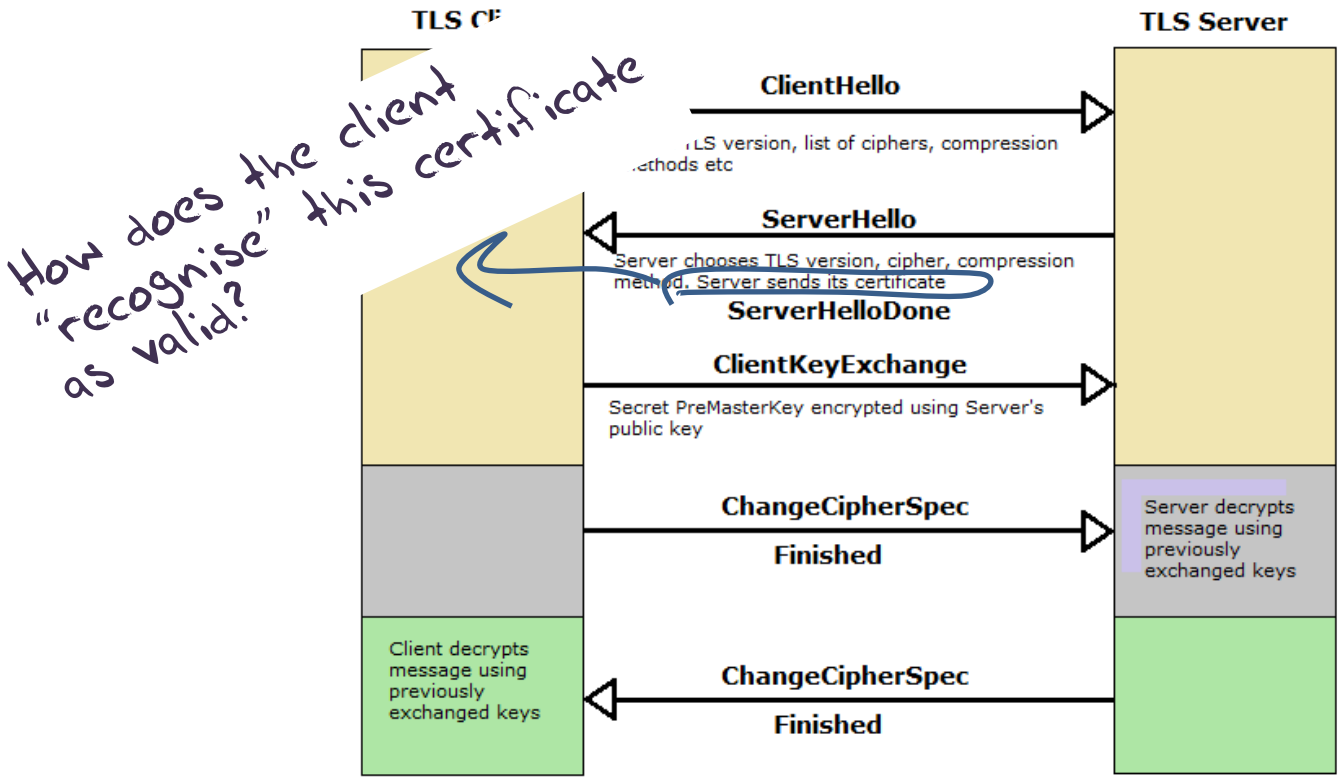
How can my browser tell the difference between an intended truth and a lie?

TLS Connections

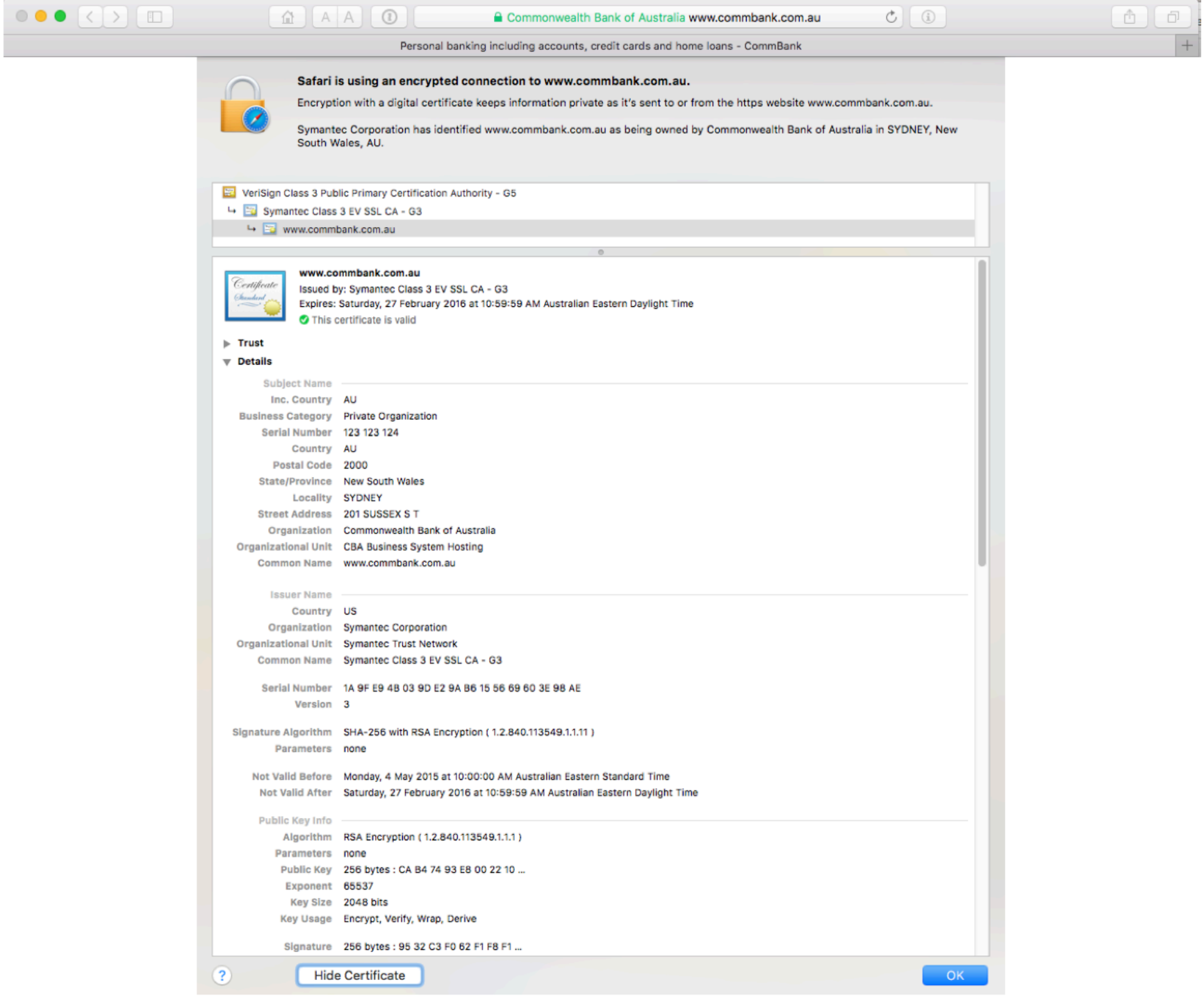


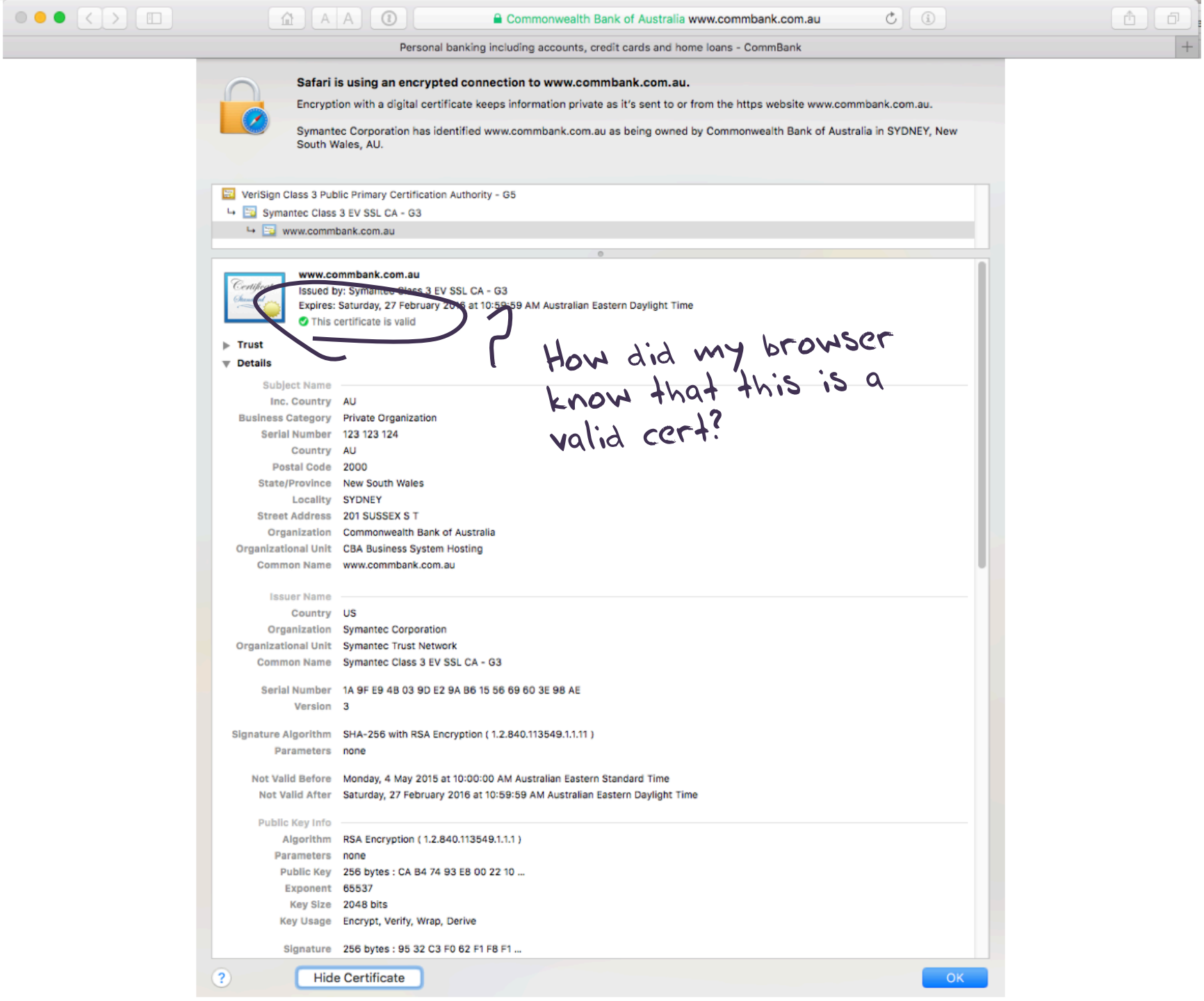
https://rhsecurity.wordpress.com/tag/tls/

TLS Connections



https://rhsecurity.wordpress.com/tag/tls/


Commonwealth Bank of Australia www.commbank.com.au
Personal banking including accounts, credit cards and home loans - CommBank
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 (1.2.840.113549.1.1.11)
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


Commonwealth Bank of Australia www.commbank.com.au
Personal banking including accounts, credit cards and home loans - CommBank
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
How did my browser know that this is a valid cert?
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 (1.2.840.113549.1.1.11)
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

Domain Name Certification

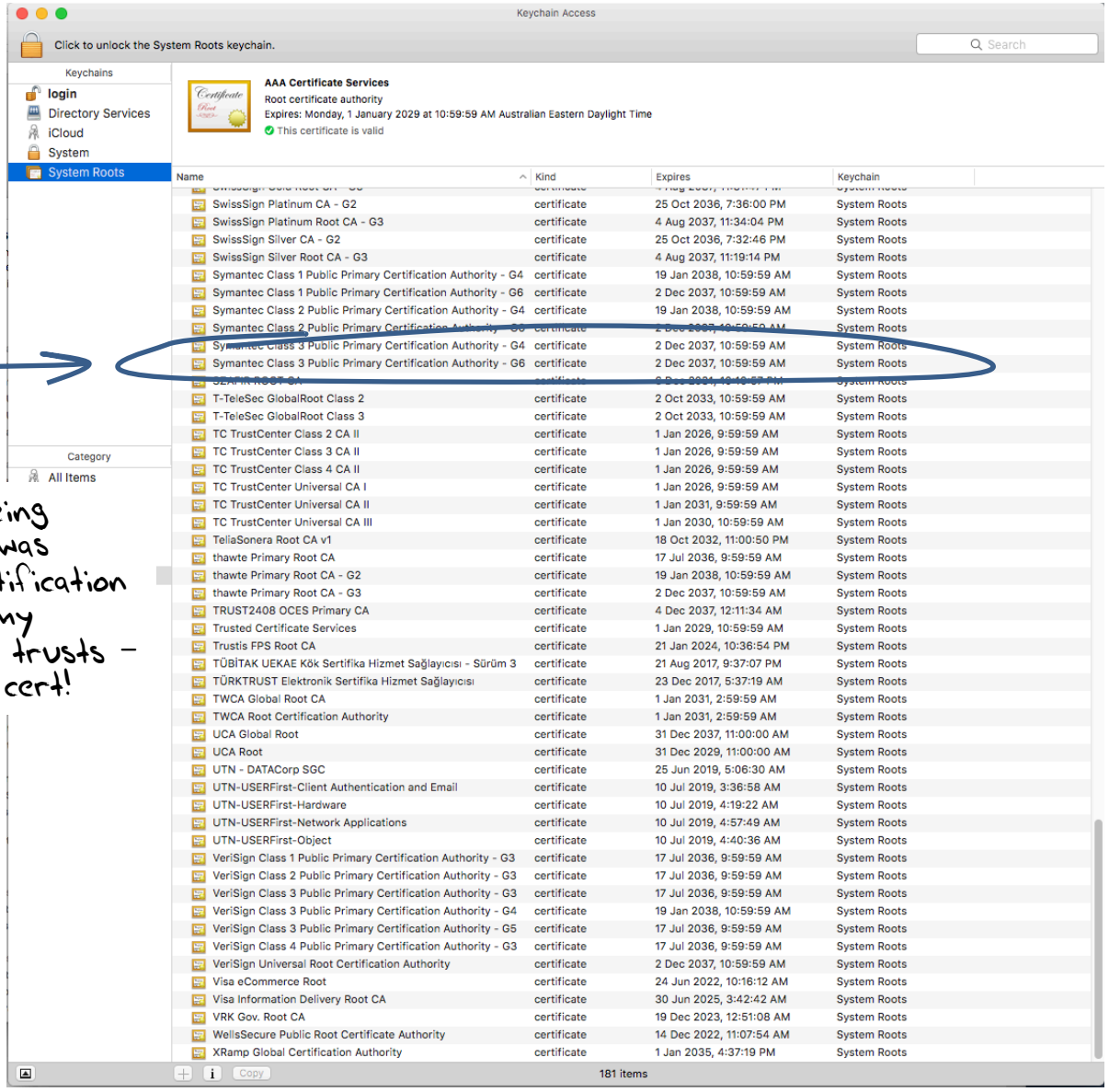
- The Commonwealth Bank of Australia has generated a key pair
- And they passed a Certificate Signing Request to a company called "Symantec" (together with money)
- Symantec is willing to vouch (in a certificate) that the entity who goes by the domain name of www.commbank.com.au also has a certain public key value (partly because it got paid to do this!)
- So if I can associate this public key with a connection then I have a high degree of confidence that I've connected to the "real" www.commbank.com.au, as long as I am also prepared to trust Symantec, and their certificate issuance processes, and that the certificates that they issue are always genuine

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" (together with money)
- Symantec 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 (partly because it got paid to do this!)
- So if I can associate this public key with a connection then I have a high degree of confidence that I've connected to the "real" www.commbank.com.au, as long as I am also prepared to trust Symantec, and their certificate issuance processes, and that the certificates that they issue are always genuine

Why should i trust them?

Local Trust

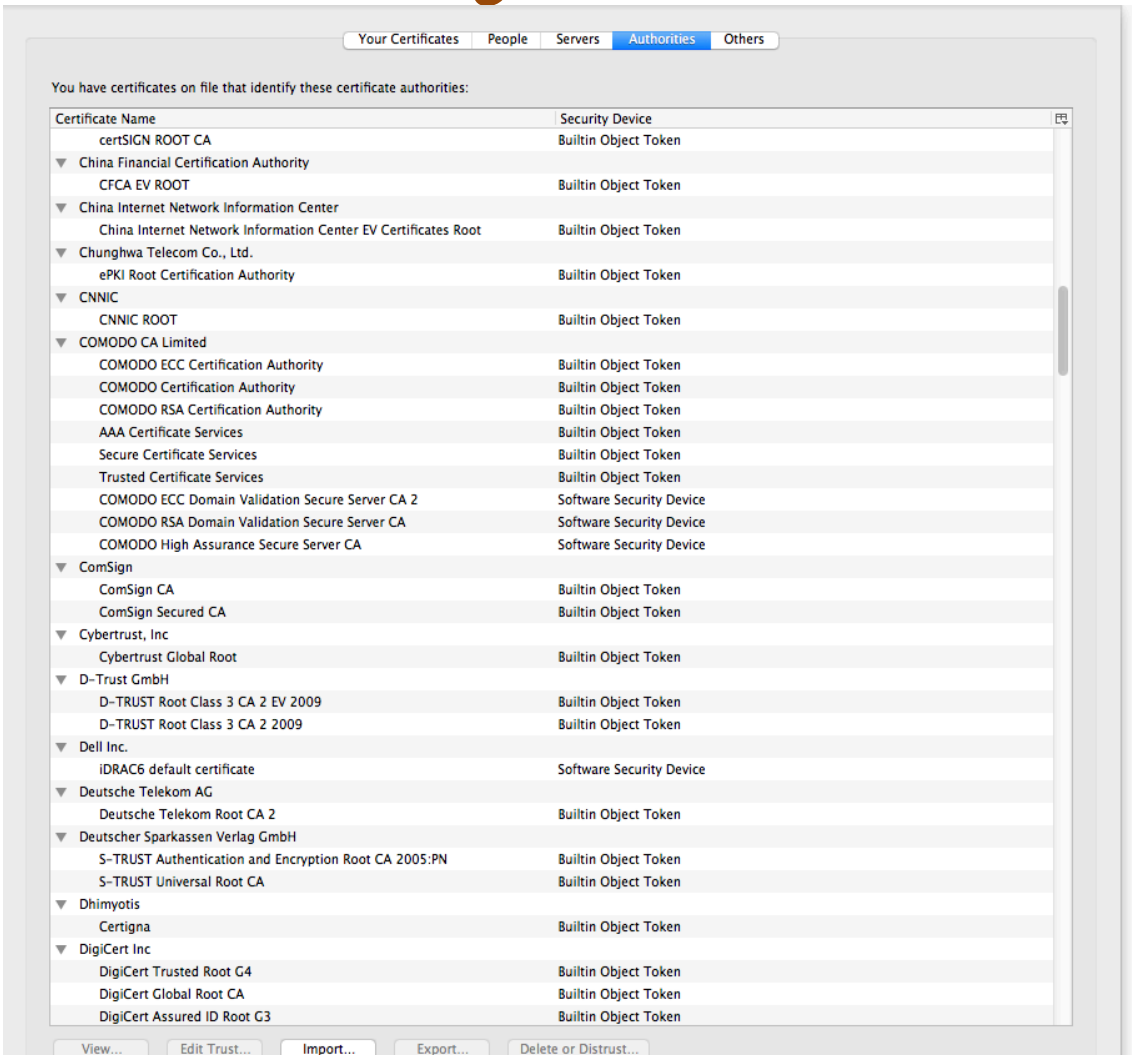


The cert I'm being asked to trust was issued by a certification authority that my browser already trusts - so I trust that cert!

Local Trust or Local Credulity*?

That's a big list of people to Trust

Are they all trustable?



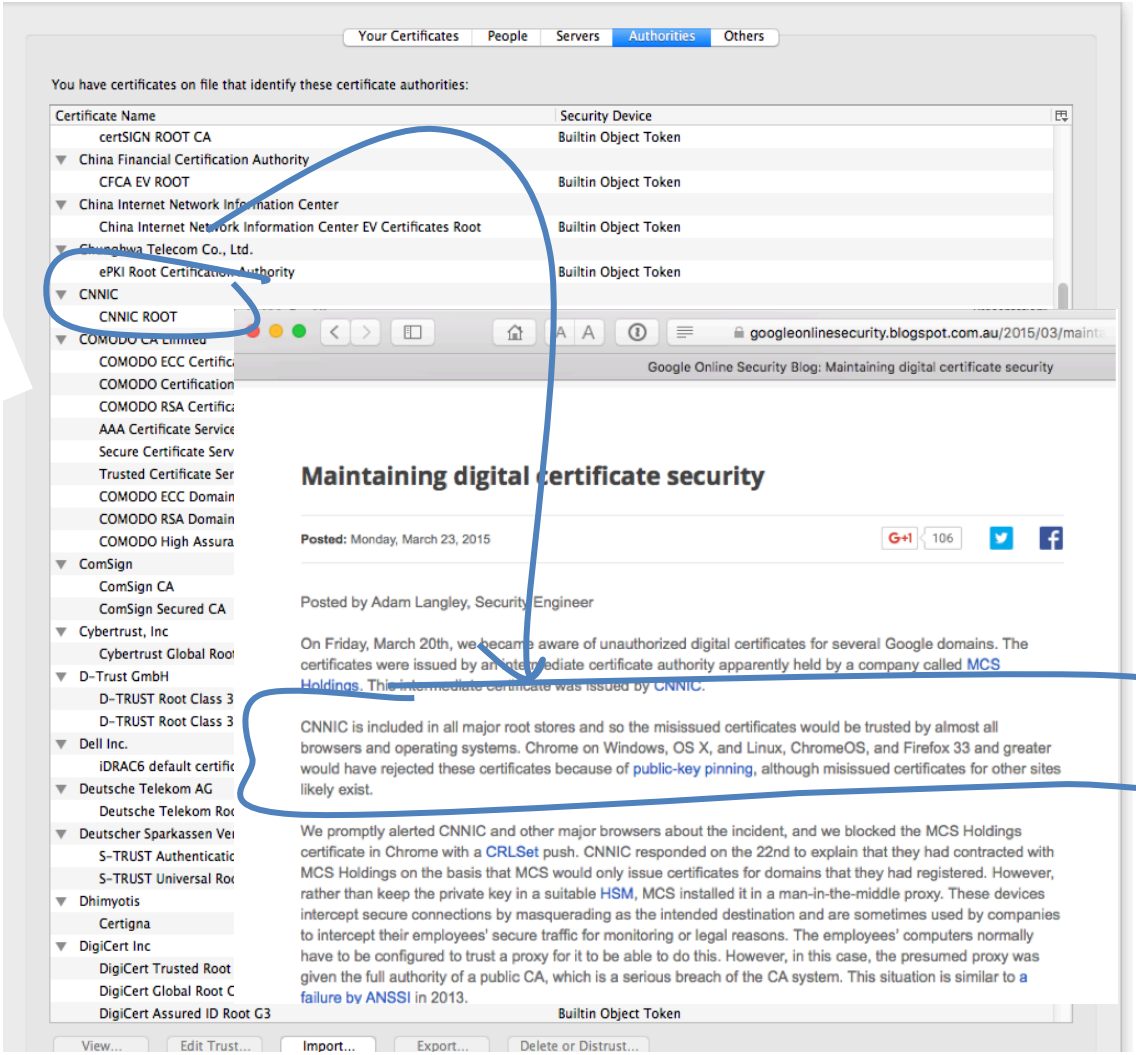
* cre·du·li·ty
/krəˈd(y)o͞olədē/
noun
a tendency to be too ready to believe that something is real or true.

Local Credulity

That's a big list of people to Trust

Are they all trustable?

Evidently Not!

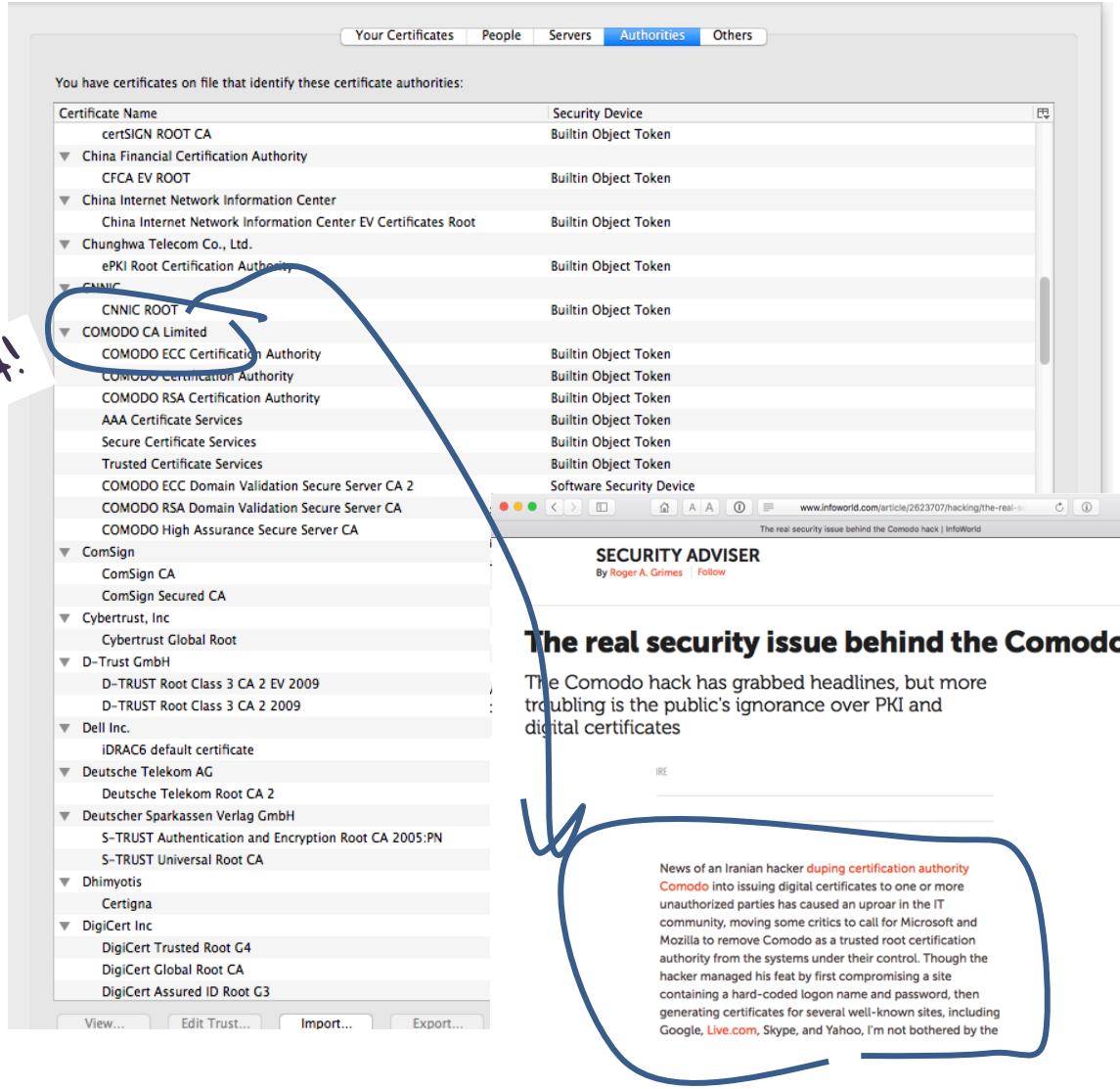


Local Credulity

That's a big list of people to Trust

Are they all trustable?

Evidently Not!



With unpleasant consequences when it all goes wrong

talk
ow

Cuba aimed at U.S.
her husband not to
anything happens,
tay right here with
told him in October
be with you, and I
u, and the children
ithout you."
nterview conducted
e of only three that
after Mr. Kennedy's
ublished as a

sters helped ignited
untry's 45-member

ing 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

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

BY SOMINI SENGUPTA

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 systems of a security firm on the outskirts of Amsterdam. He created fake credentials 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 ed to tap into the online many as 300,000 ummer.

online security mechanism that is trusted by Internet users all over the world.

Comodohacker, as he calls himself, insists that he acted on his own and is unperturbed 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 resp

In th
is most
reckon
HACKER,

net attacks, this
ment of

International Herald Tribune
Sep 13, 2011 Front Page

What's going wrong here?

- The TLS handshake cannot specify WHICH CA should be used to validate the digital certificate
- That means that your browser may 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 the digital certificate
- That means that your browser may allow ANY CA to be used to validate a certificate

WOW! That's awesomely bad!

What's going wrong here?

- The TLS handshake cannot specify WHICH CA shou
  c
- That
  CA to be used t

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

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

ANY

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/DefconSSLiverse.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?

?

In a commercial environment

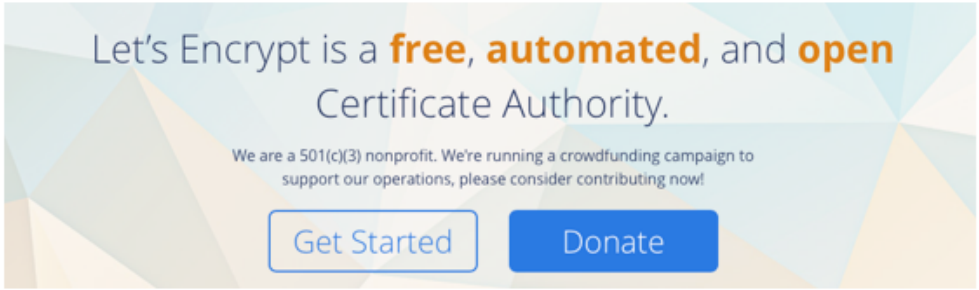
Where CA's compete with each other for market share

And quality offers no protection

Than what 'wins' in the market?

Where now?

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



www.letsencrypt.org

Where now?

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

Will the automation of the Cert issuance coupled with a totally free service make the overall environment more or less secure?

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

Where now?

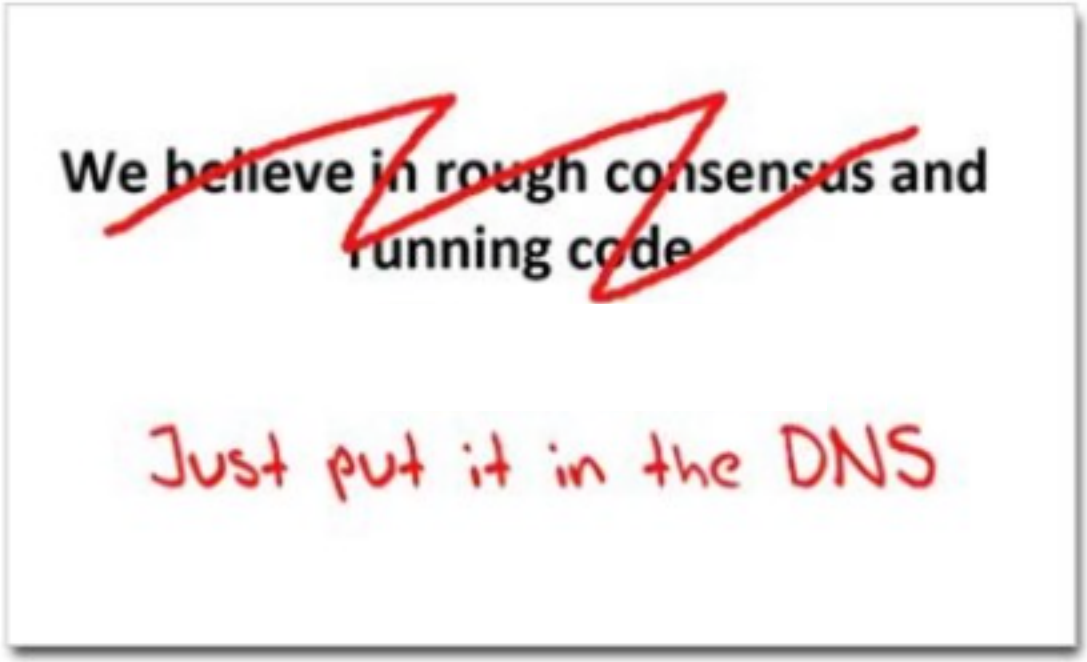
Option B: White Listing and Pinning with HSTS

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

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

Where now?

Option C: Use the DNS!



cafepress.com/nxdomain

Seriously … just use the DNS Luke!*

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

* Ok, that was a cheap shot – my apologies to the Star Wars franchise!

Seriously

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

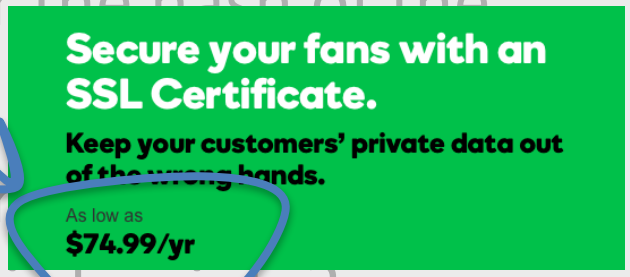
- Why not query the DNS for the HSTS record?
- Why not query the DNS for the issuer CA?
- Why not query the DNS for the hash of the domain name cert?
- Why not query the DNS for the hash of the domain name subject public key info?

Seriously

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

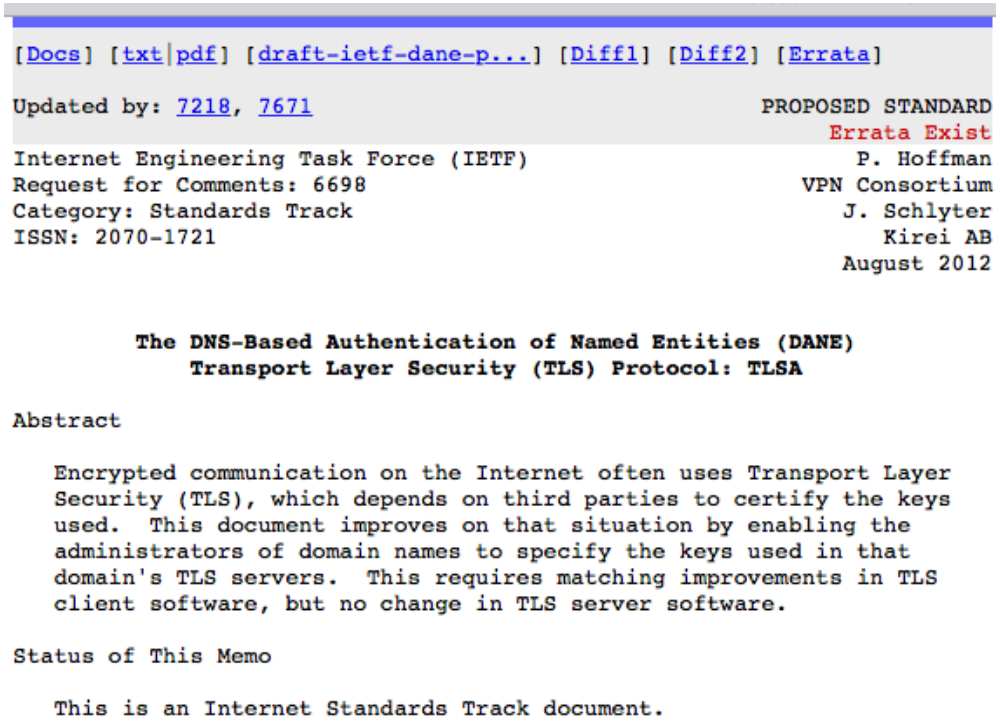
- Why not quer… the HSTS record?
- W… the DNS for the issuer CA?
- Why not query the DNS for the hash of the domain name cert?
- Why not query the DNS for … name subject public key info?

Who needs CA's anyway?



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, Errata Exist

Internet Engineering Task Force (IETF) — P. Hoffman, VPN Consortium
Request for Comments: 6698 — J. Schlyter, Kirei AB
Category: Standards Track — August 2012
ISSN: 2070-1721

The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA

Abstract

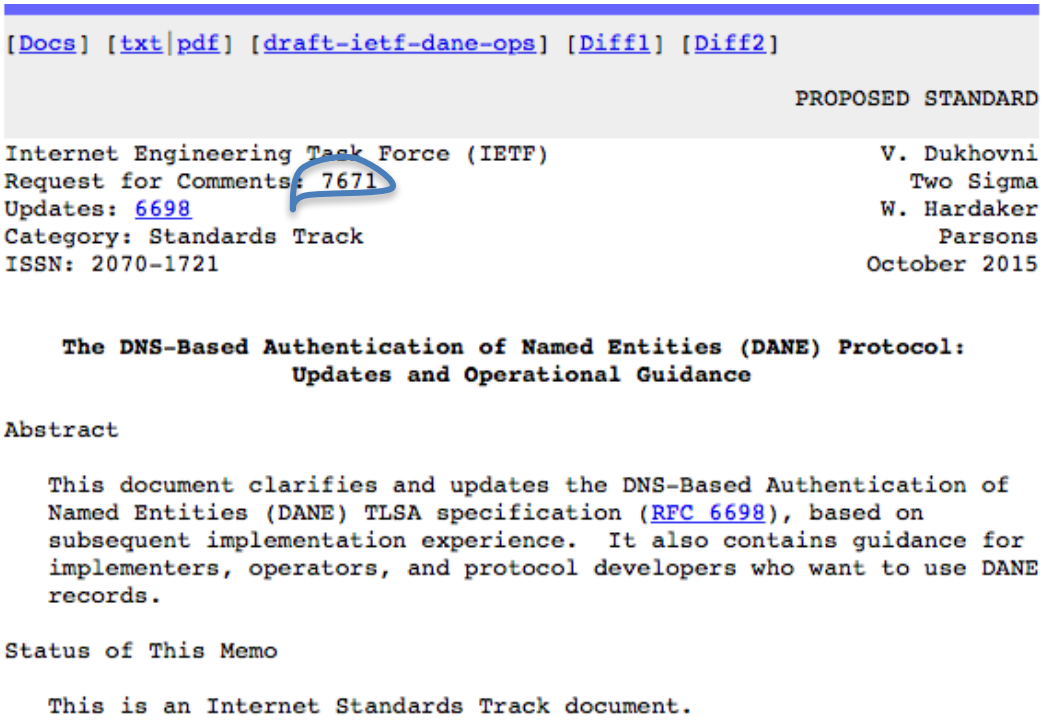
Encrypted communication on the Internet often uses Transport Layer Security (TLS), which depends on third parties to certify the keys used. This document improves on that situation by enabling the administrators of domain names to specify the keys used in that domain's TLS servers. This requires matching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

Status of This Memo

This is an Internet Standards Track document.

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 — Parsons
ISSN: 2070-1721 — October 2015

The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance

Abstract

This document clarifies and updates the DNS-Based Authentication of Named Entities (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.

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
          7983a1d16e8a410e4561cb106618e971 )
```

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:

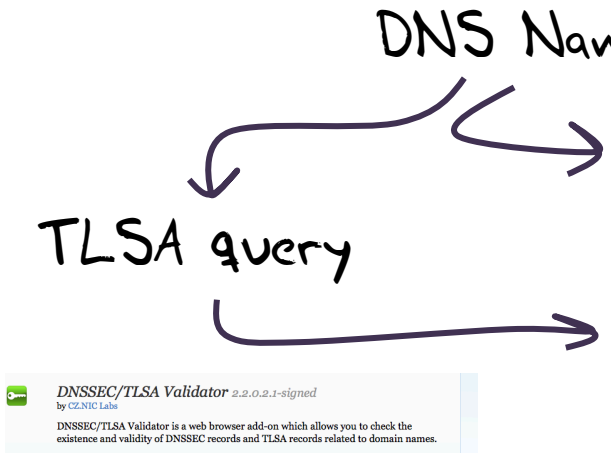
```
_443._tcp.www.example.com. IN TLSA
    2 0 0 30820307308201efa003020102020... )
```

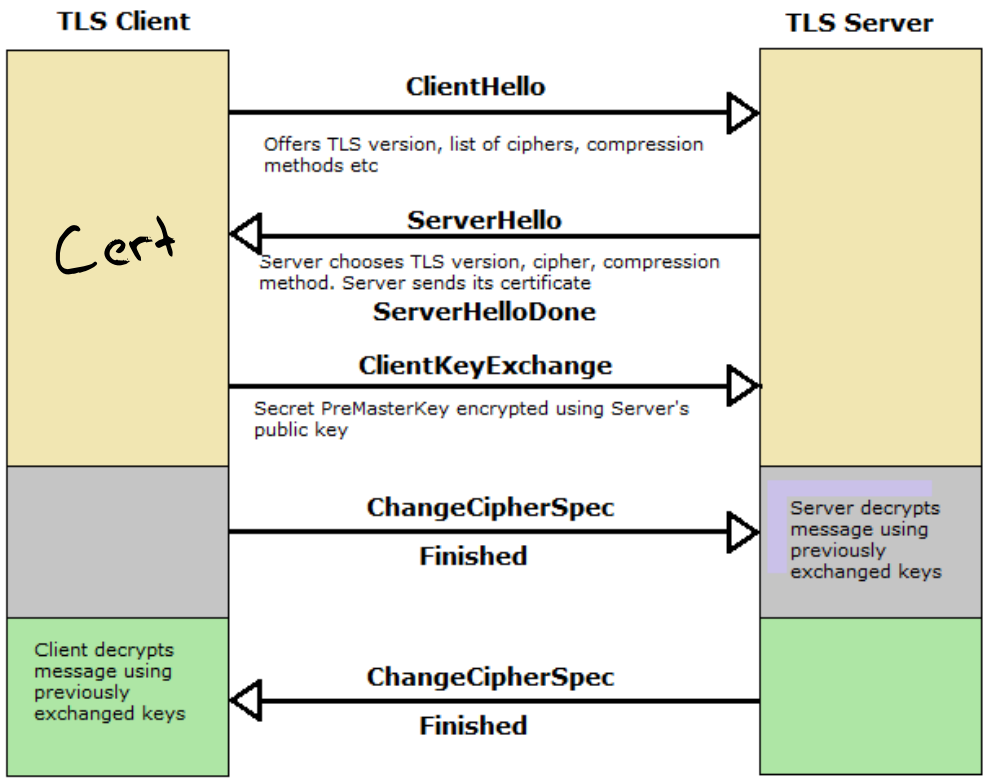
Trust Anchor

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





https://rhsecurity.wordpress.com/tag/tls/

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

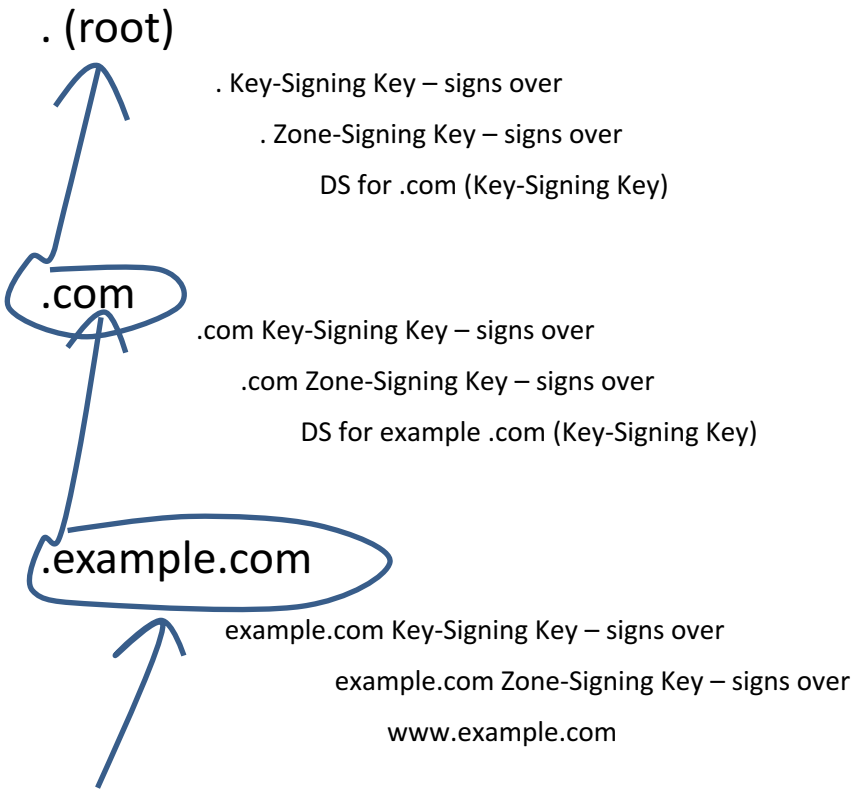
example.com Key-Signing Key – signs over

example.com Zone-Signing Key – signs over

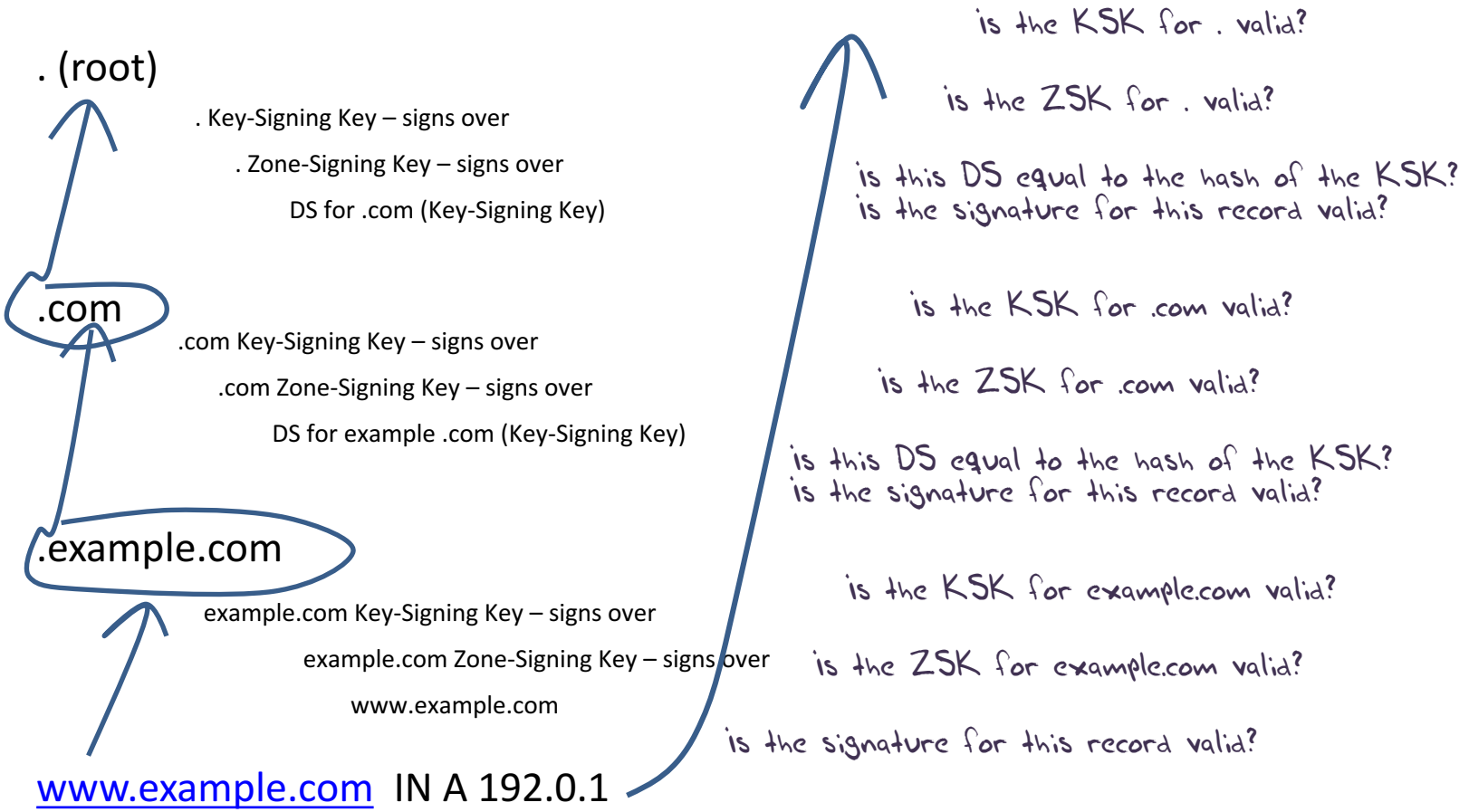
www.example.com

www.example.com

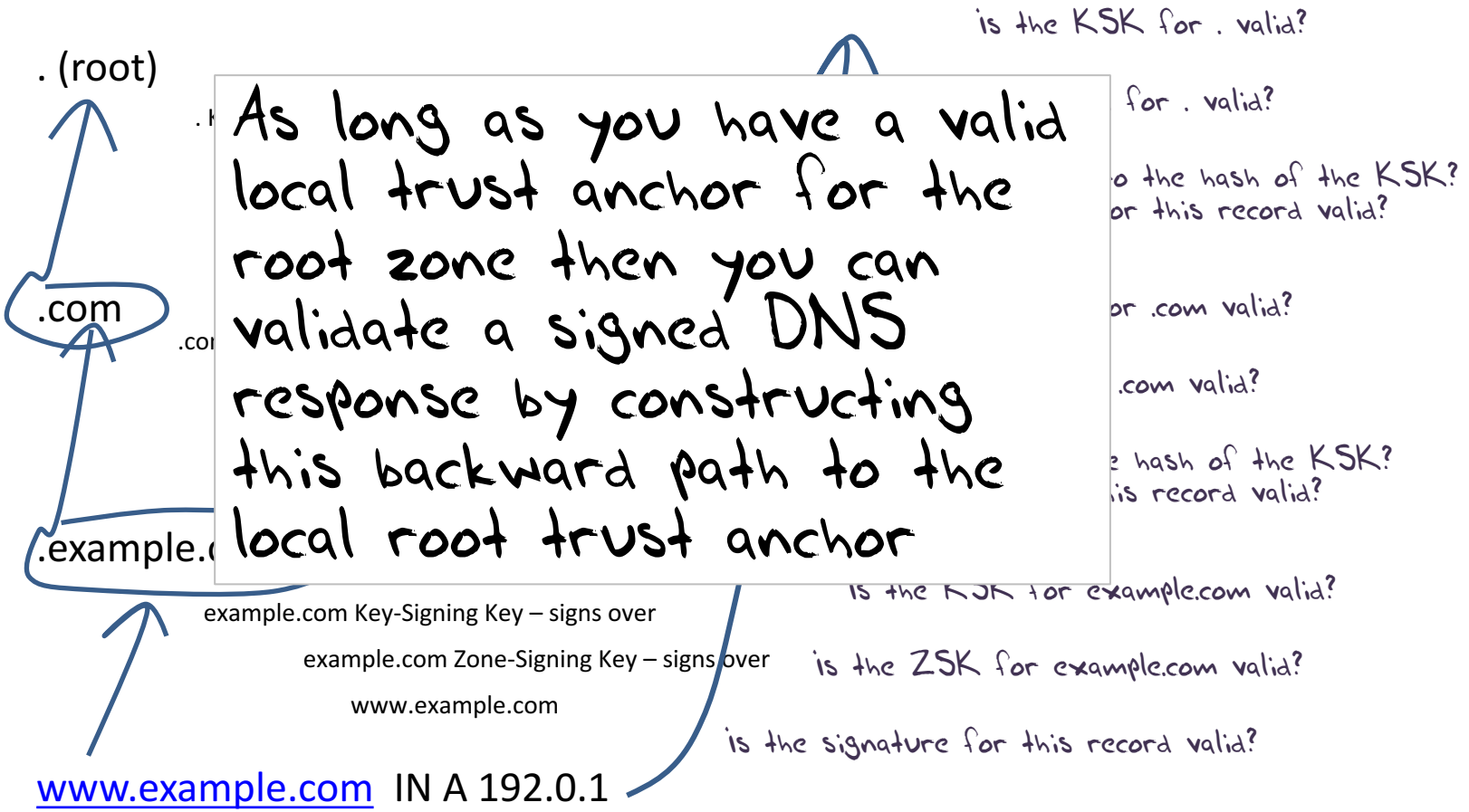
DNSSEC Interlocking Signatures



DNSSEC Interlocking Signatures



DNSSEC Interlocking Signatures



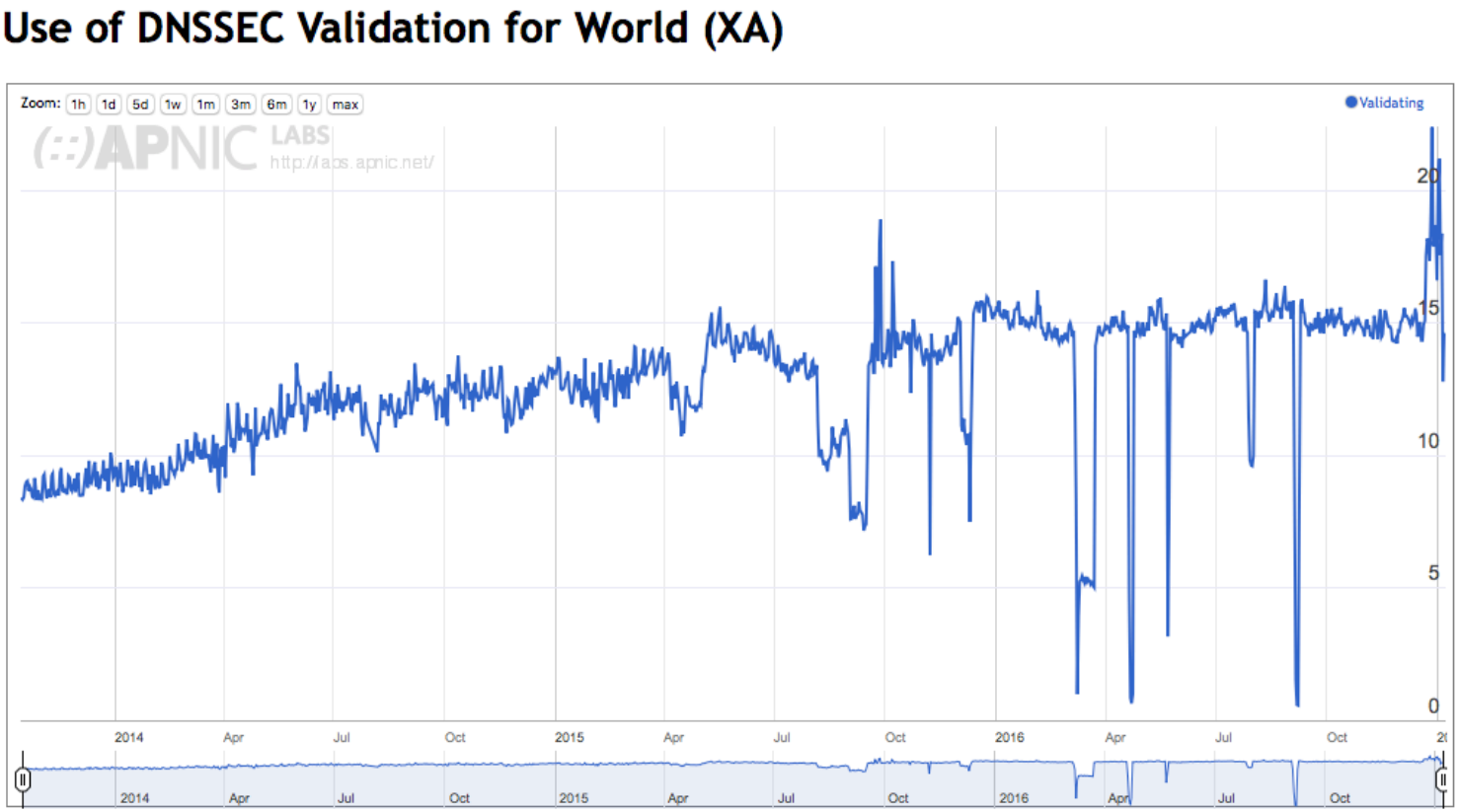
DANE + DNSSEC

- 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

So we need DNSSEC as well as DANE…

How much DNSSEC Validation is out there?

Do we do DNSSEC Validation?



stats.labs.apnic.net/dnssec/XA

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

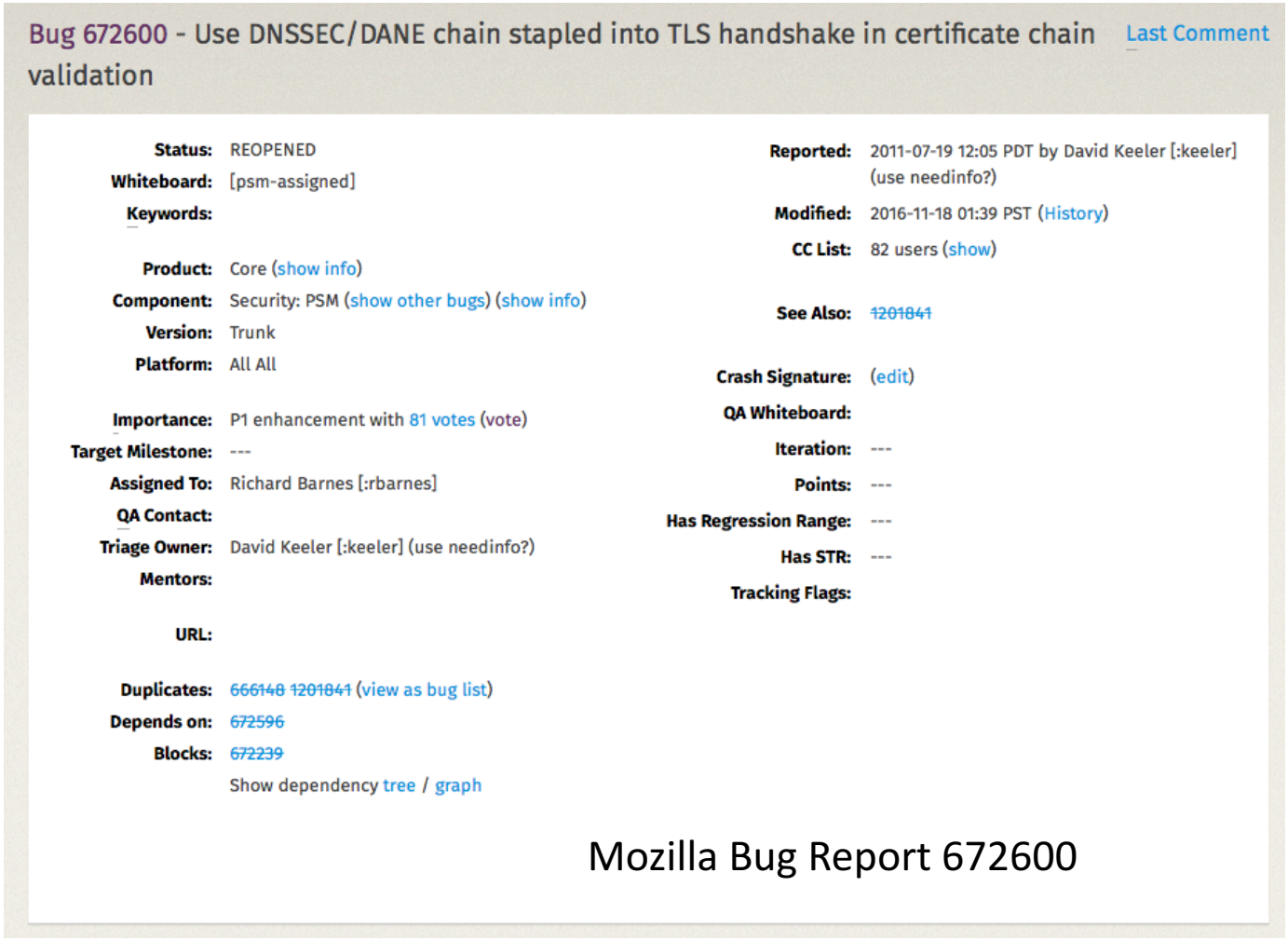
Where now?

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!

Maybe this will change



Bug 672600 - Use DNSSEC/DANE chain stapled into TLS handshake in certificate chain validation Last Comment

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)		
Component:	Security: PSM (show other bugs) (show info)	**See Also:**	~~1201841~~
Version:	Trunk		
Platform:	All All	**Crash Signature:**	(edit)
		QA Whiteboard:	
Importance:	P1 enhancement with 81 votes (vote)	**Iteration:**	---
Target Milestone:	---	**Points:**	---
Assigned To:	Richard Barnes [:rbarnes]	**Has Regression Range:**	---
QA Contact:		**Has STR:**	---
Triage Owner:	David Keeler [:keeler] (use needinfo?)	**Tracking Flags:**	
Mentors:			
URL:			
Duplicates:	~~666148~~ ~~1201841~~ (view as bug list)		
Depends on:	~~672596~~		
Blocks:	~~672239~~		
	Show dependency tree / graph		

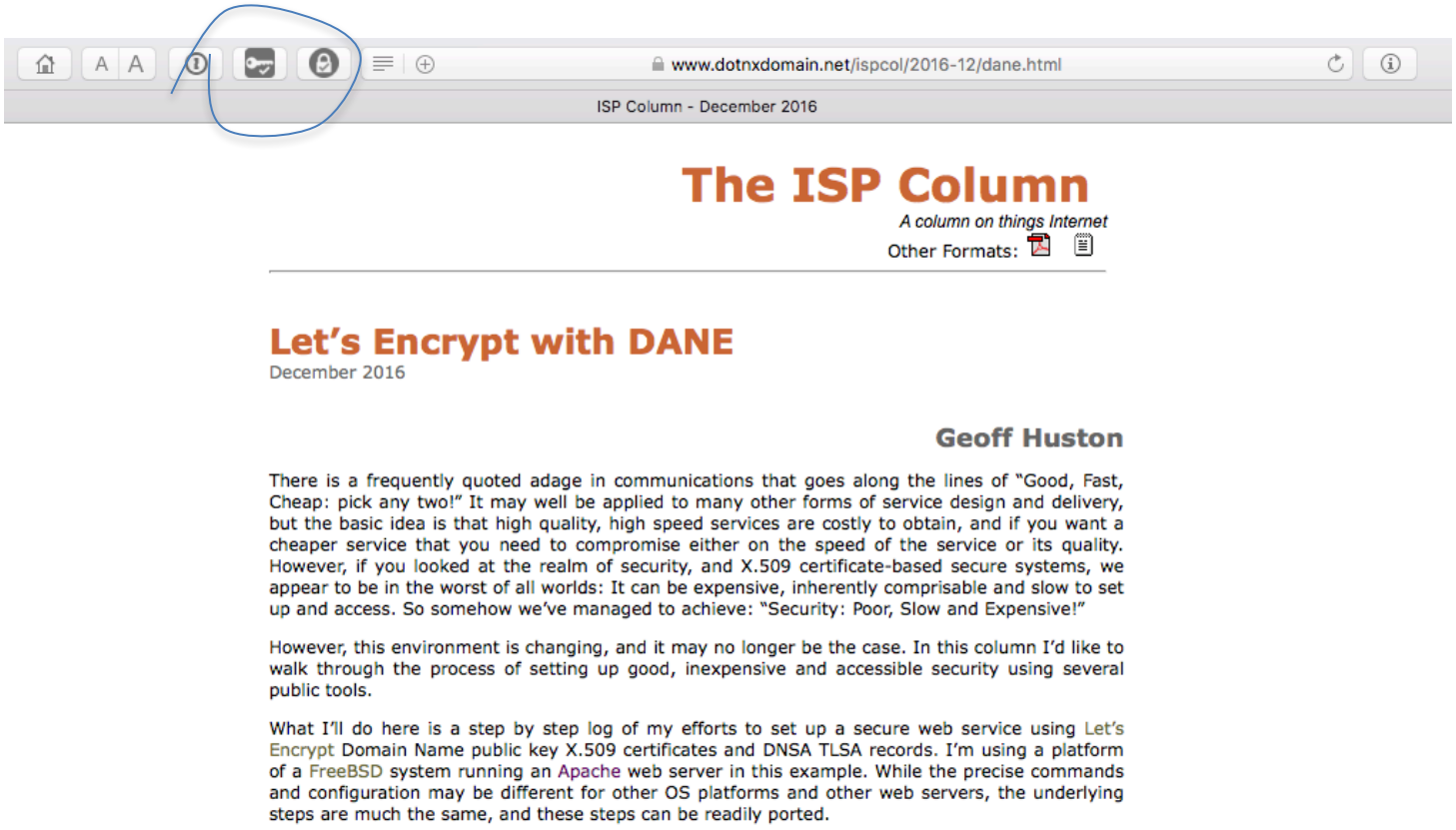
Mozilla Bug Report 672600

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 Key Exchange for TLS

Let's Do it!



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?