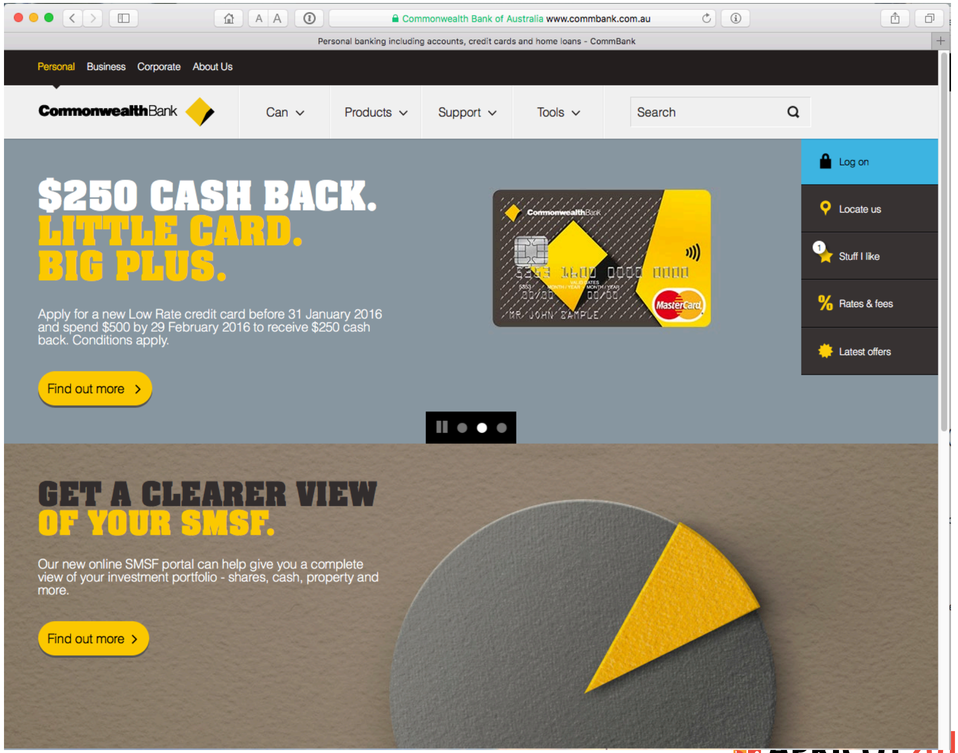
Why Dane?

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?



Commonwealth Bank of Australia www.commbank.com.au

Personal banking including accounts, credit cards and home loans - CommBank

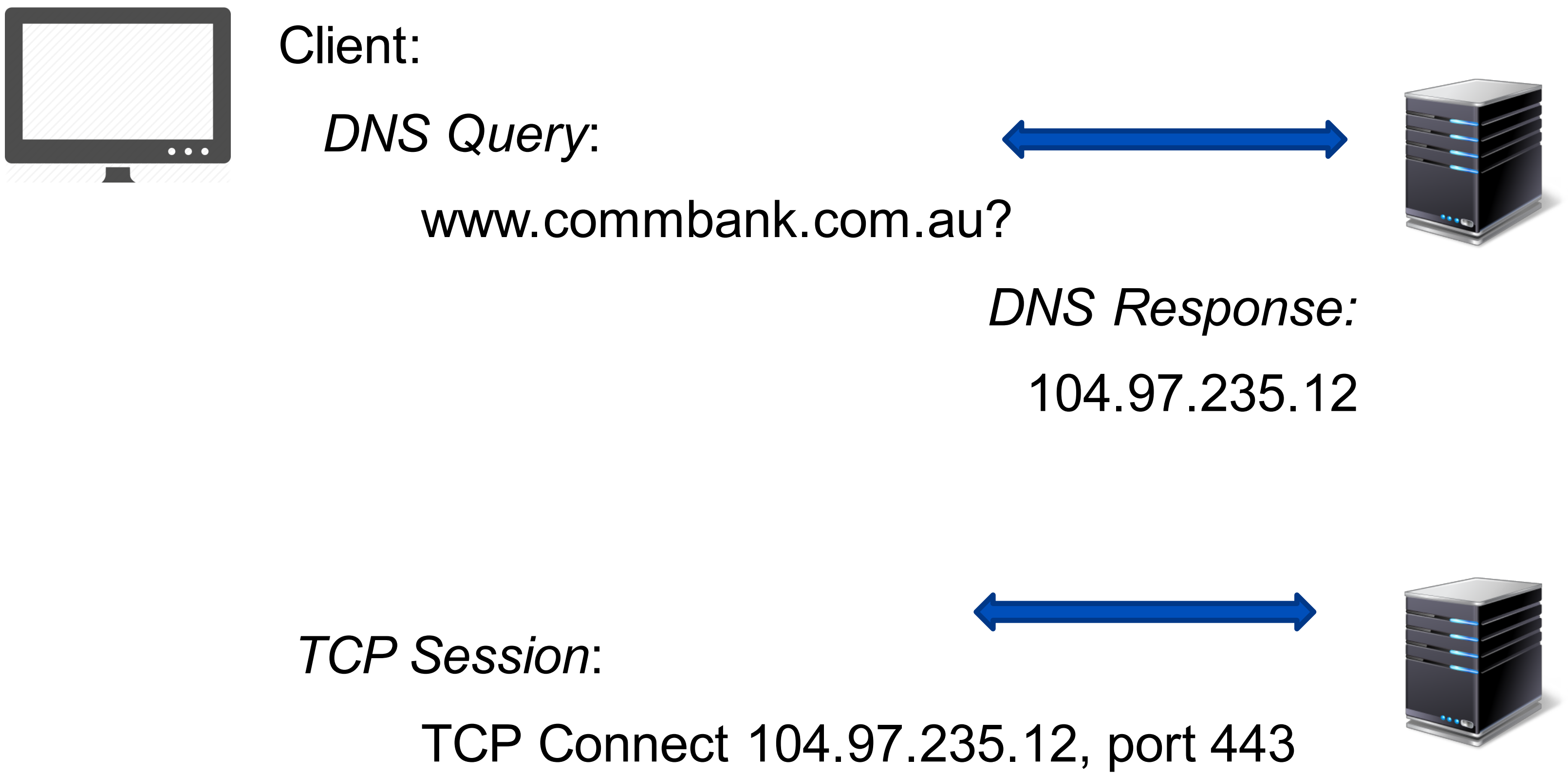
$250 CASH BACK.
LITTLE CARD.
BIG PLUS.

Apply for a new Low Rate credit card before 31 January 2016 and spend $500 by 29 February 2016 to receive $250 cash back. Conditions apply.

GET A CLEARER VIEW
OF YOUR SMSF.

Our new online SMSF portal can help give you a complete view of your investment portfolio - shares, cash, property and more.

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.
```

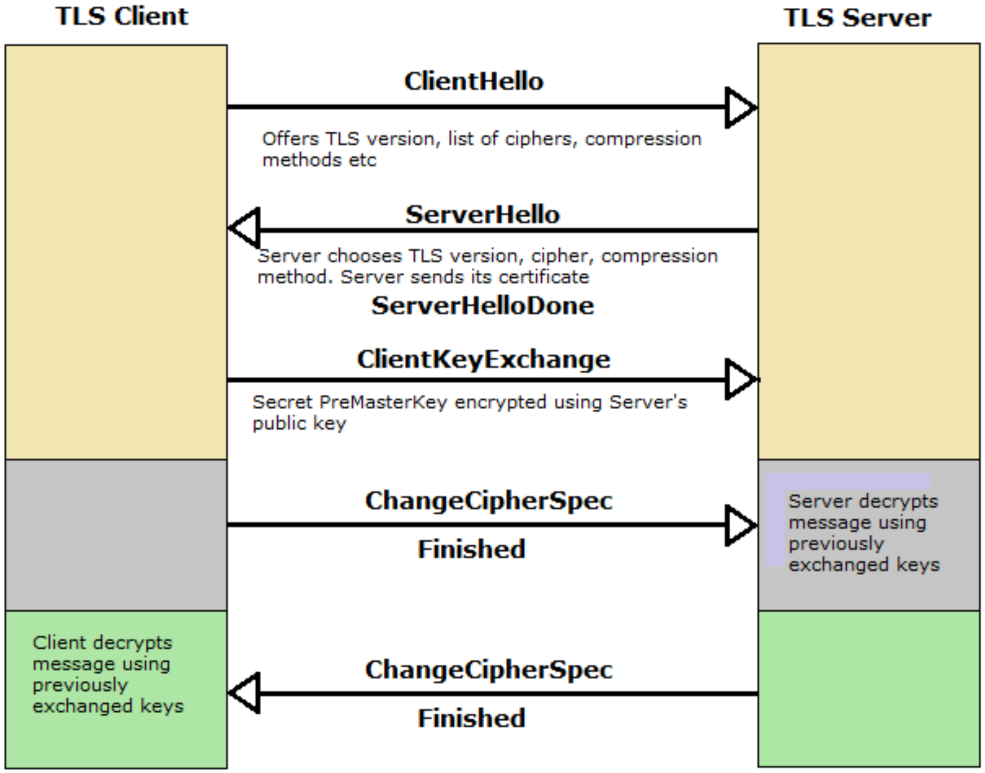
That’s not an IP addresses that was allocated to the Commonwealth Bank!

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



TLS Client

TLS Server

ClientHello

Offers TLS version, list of ciphers, compression methods etc

ServerHello

Server chooses TLS version, cipher, compression method. Server sends its certificate

ServerHelloDone

ClientKeyExchange

Secret PreMasterKey encrypted using Server's public key

ChangeCipherSpec

Finished

Server decrypts message using previously exchanged keys

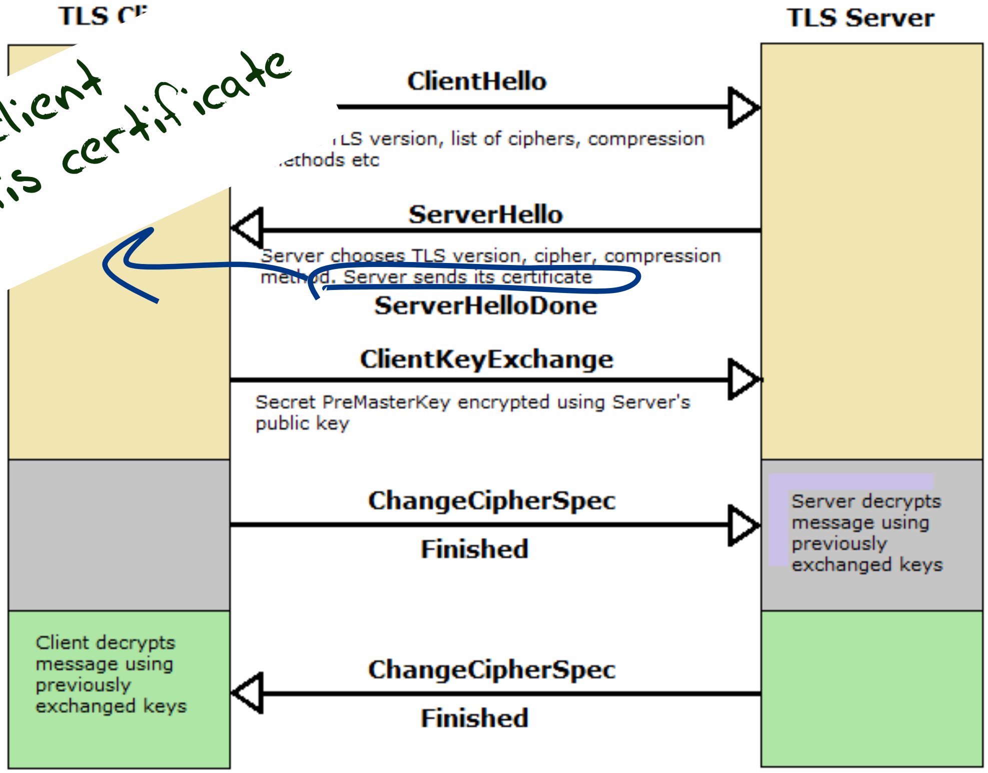
Client decrypts message using previously exchanged keys

ChangeCipherSpec

Finished

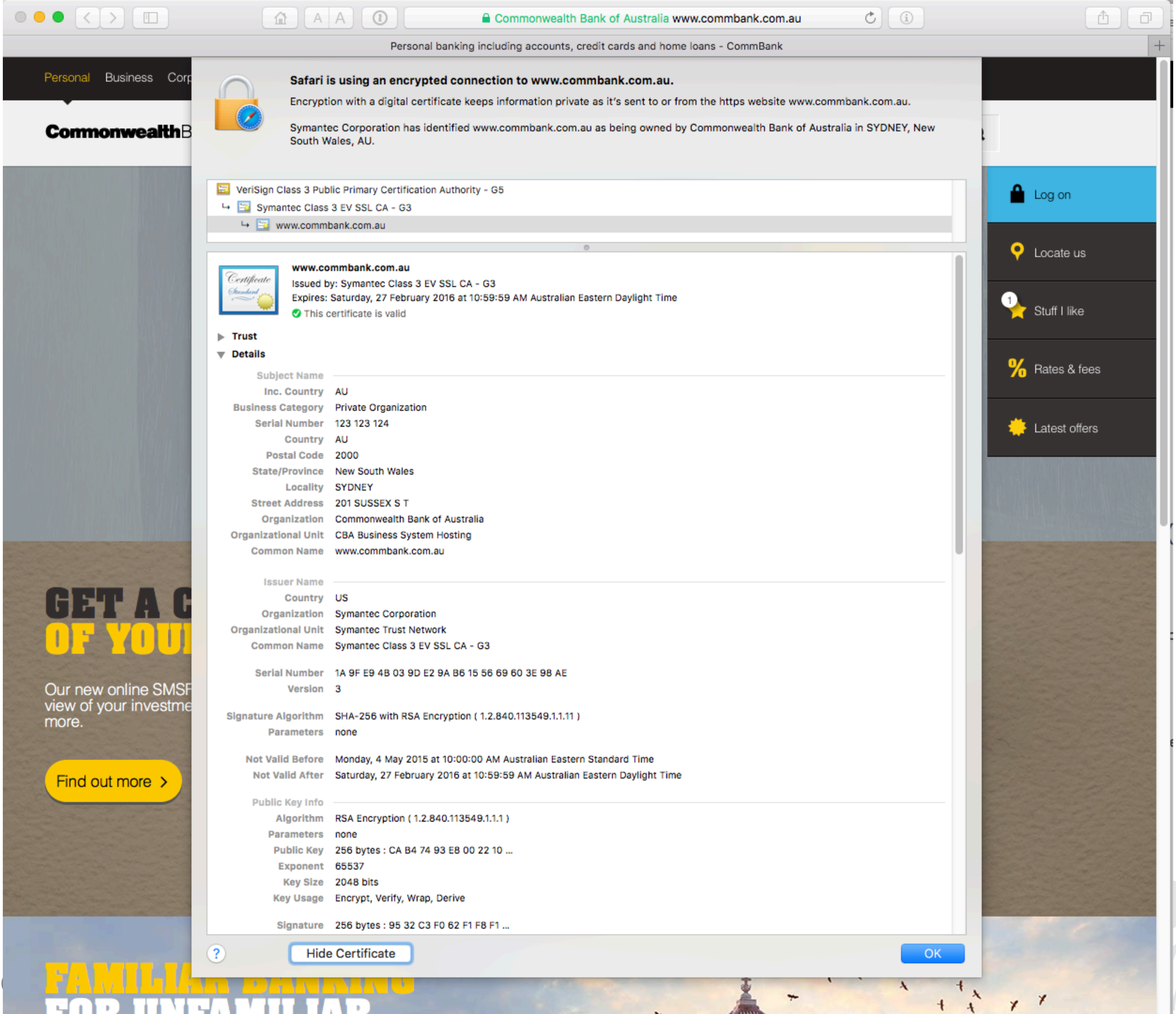
https://rhsecurity.wordpress.com/tag/tls/

TLS Connections



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

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



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

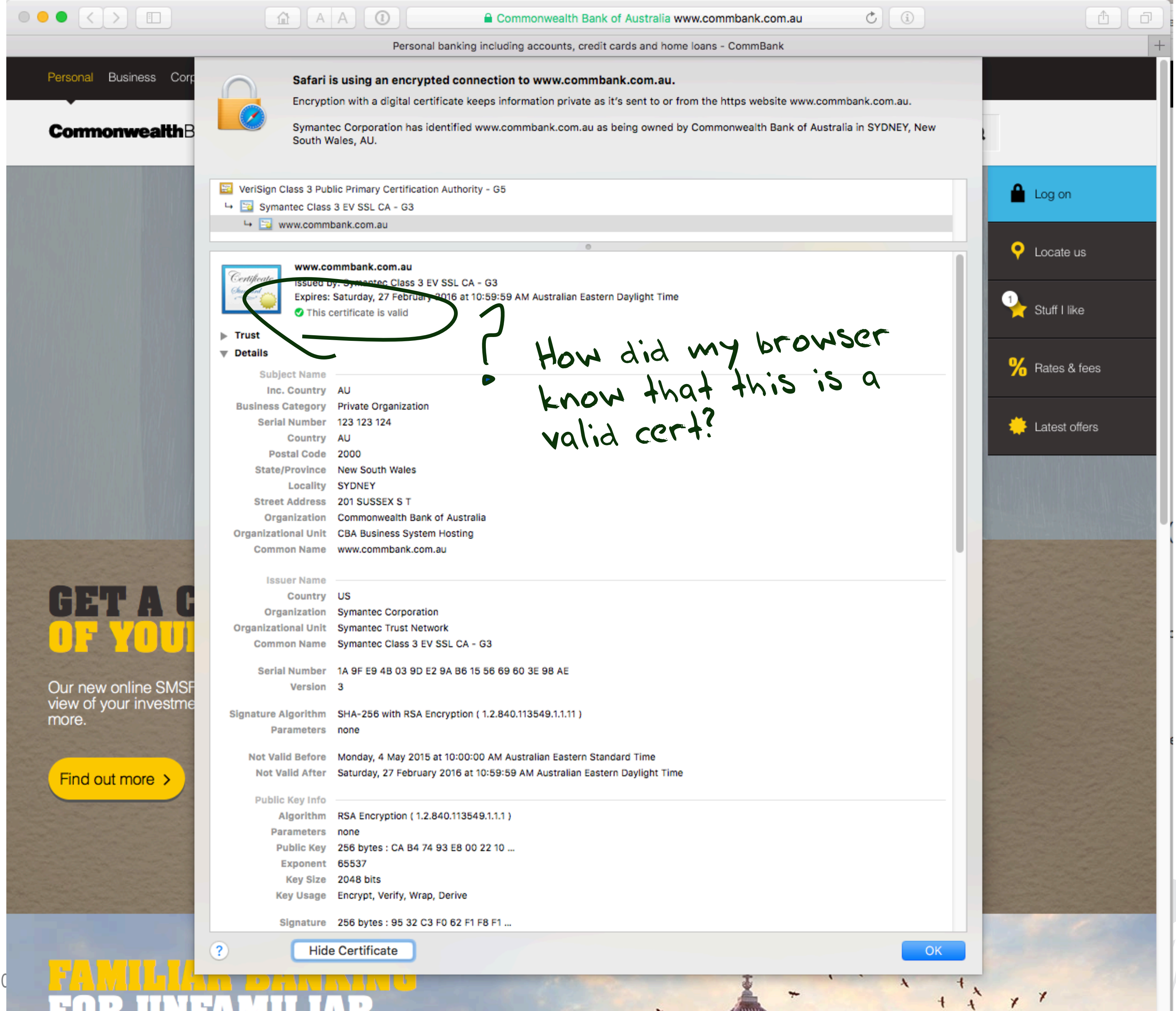
www.commbank.com.au
Issued by: Symantec Class 3 EV SSL CA - G3
Expires: Saturday, 27 February 2016 at 10:59:59 AM Australian Eastern Daylight Time
✓ This certificate is valid

▶ **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 ...

#apricot2


Commonwealth Bank of Australia www.commbank.com.au
Personal banking including accounts, credit cards and home loans - CommBank
Personal
Business
Corp
CommonwealthB
Log on
Locate us
1
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 (1.2.840.113549.1.1.11)
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 ...

?

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

Domain Name Certification

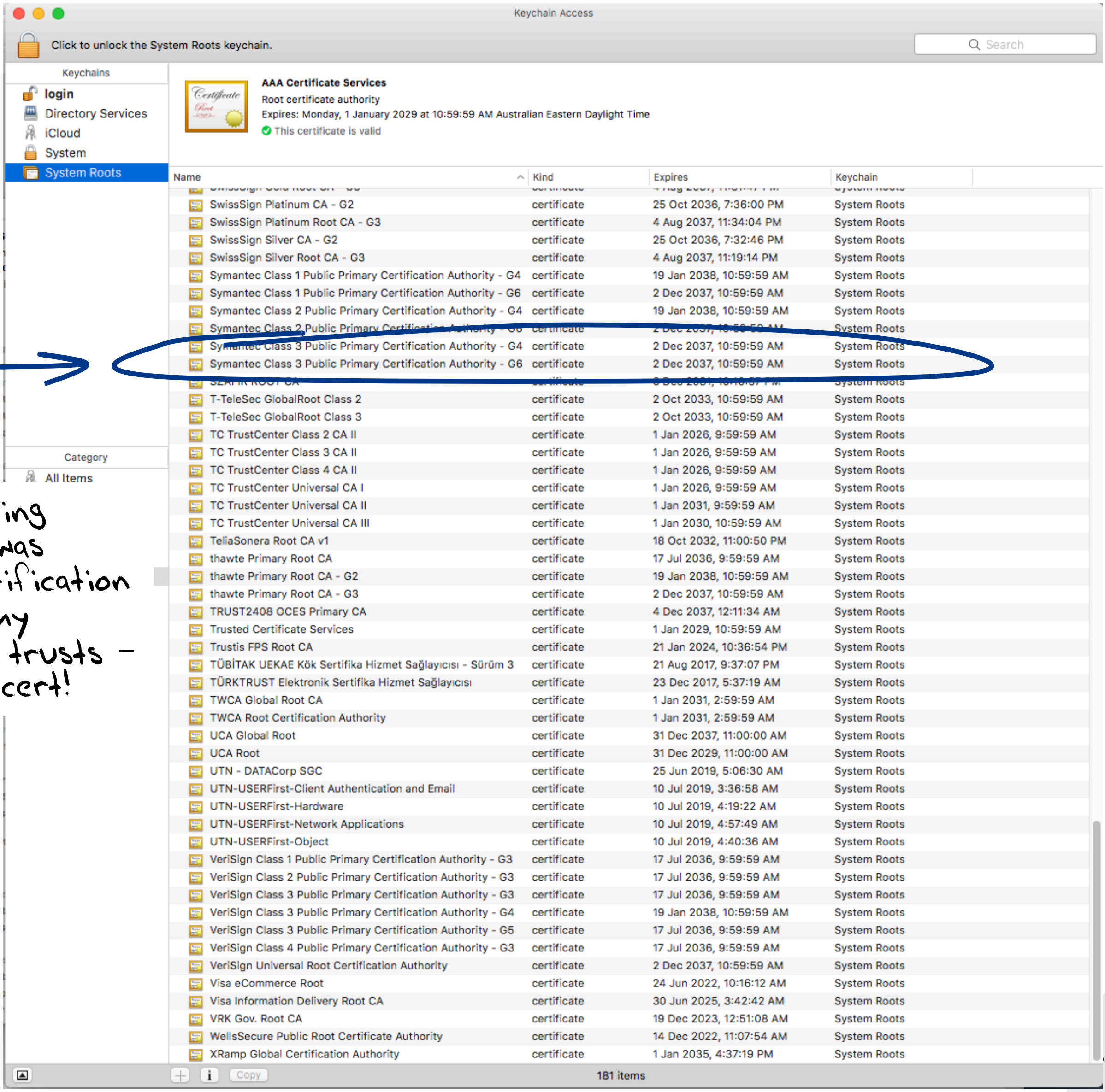
- The Commonwealth Bank of Australia has generated a key pair
- And they passed a certificate signing request to a company called “Symantec”
- Who is willing to vouch (in a certificate) that the entity who goes by the domain name of www.commbank.com.au also has a certain public key value
- So if I can 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



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

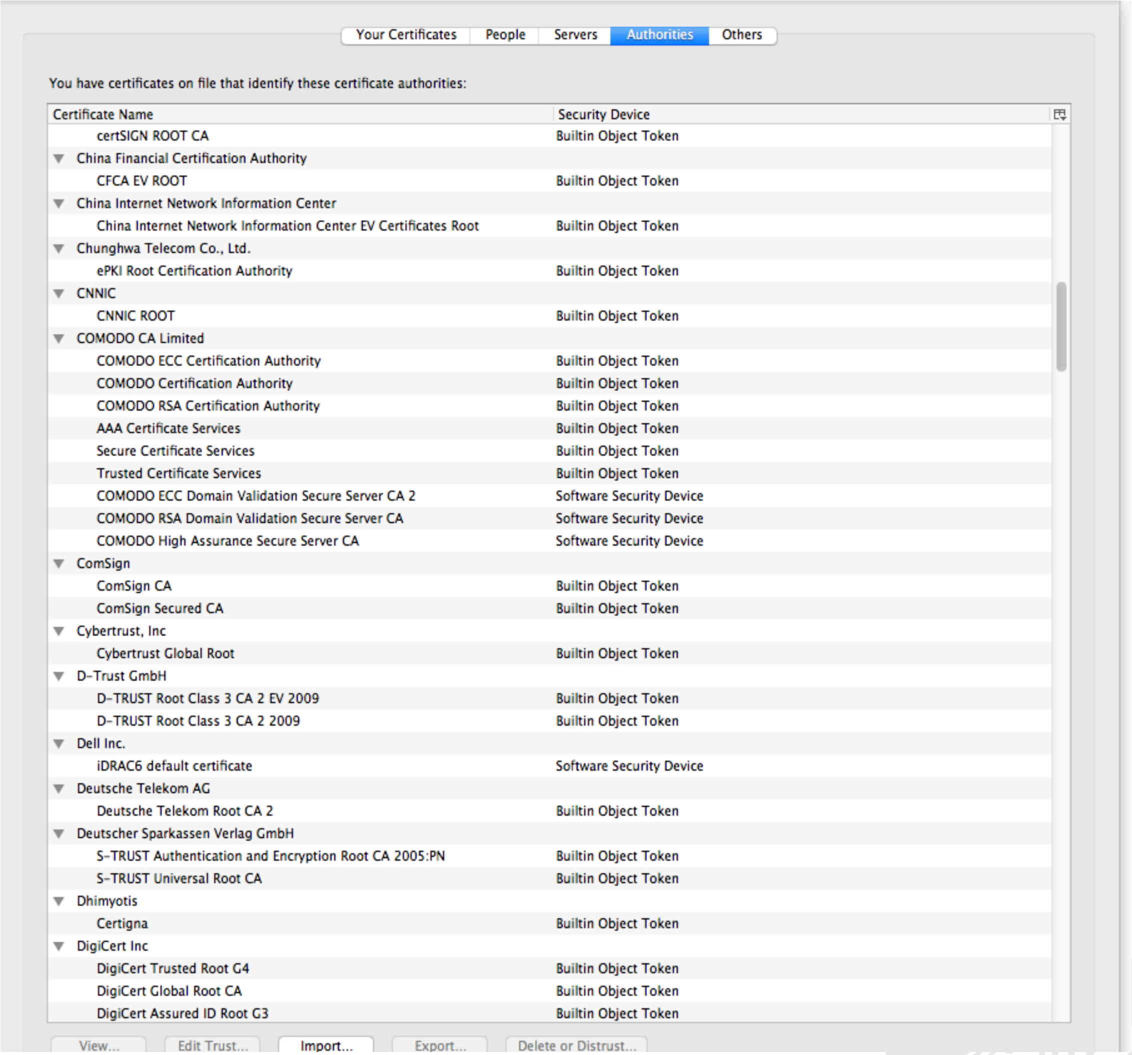
Name	Kind	Expires	Keychain
SwissSign Gold Root CA - G3	certificate	4 Aug 2037, 11:31:47 PM	System Roots
SwissSign Platinum CA - G2	certificate	25 Oct 2036, 7:36:00 PM	System Roots
SwissSign Platinum Root CA - G3	certificate	4 Aug 2037, 11:34:04 PM	System Roots
SwissSign Silver CA - G2	certificate	25 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
SZAFIR ROOT CA	certificate	6 Dec 2031, 10:10:57 PM	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
TÜRKTRUST 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

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

That’s a big list of people to Trust

Are they all trustable?



You have certificates on file that identify these certificate authorities:

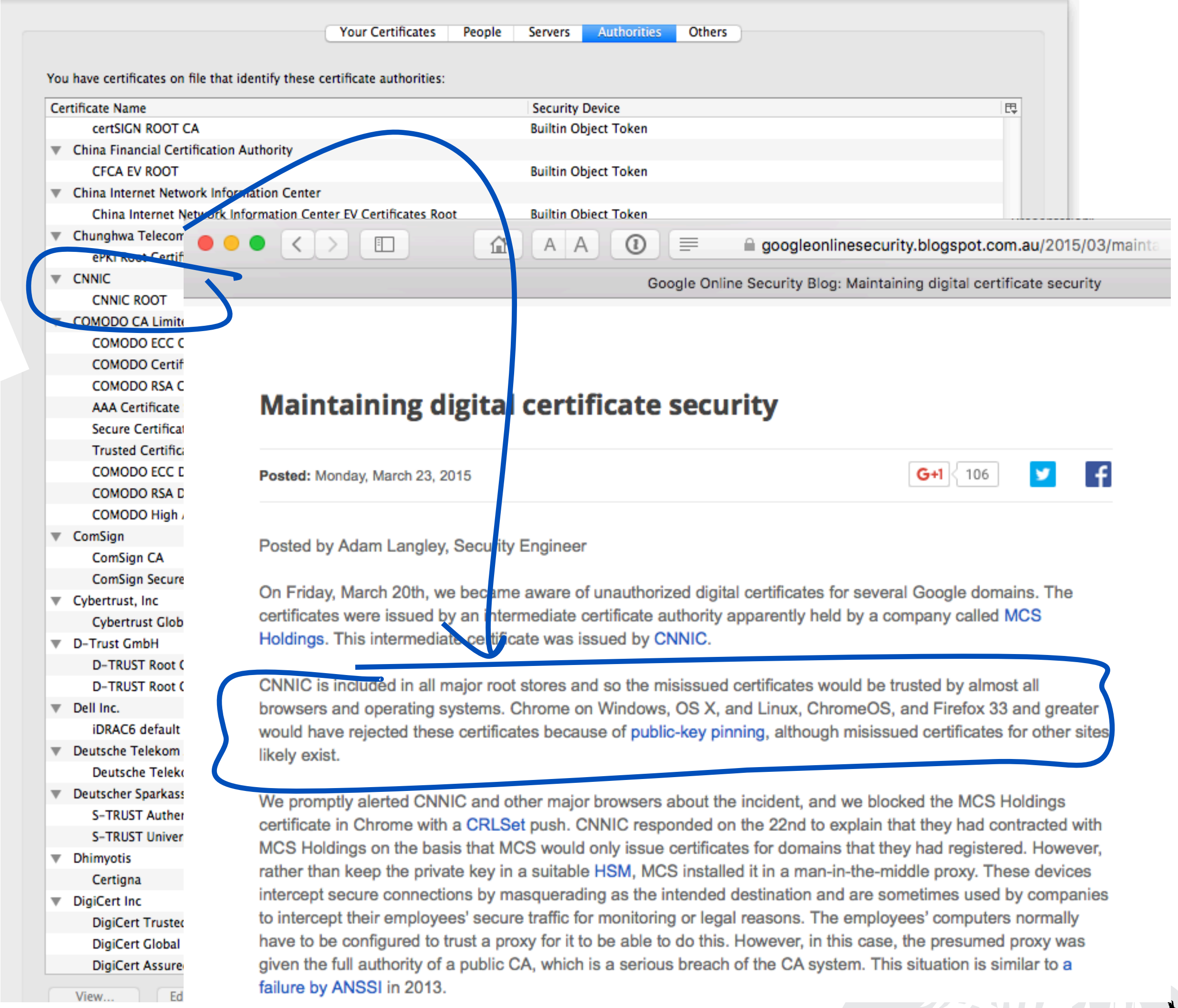
Certificate Name	Security Device
certSIGN ROOT CA	Builtin Object Token
▼ China Financial Certification Authority	
CFCA EV ROOT	Builtin Object Token
▼ China Internet Network Information Center	
China Internet Network Information Center EV Certificates Root	Builtin Object Token
▼ Chunghwa Telecom Co., Ltd.	
ePKI Root Certification Authority	Builtin Object Token
▼ CNNIC	
CNNIC ROOT	Builtin Object Token
▼ COMODO CA Limited	
COMODO ECC Certification Authority	Builtin Object Token
COMODO Certification Authority	Builtin Object Token
COMODO RSA Certification Authority	Builtin Object Token
AAA Certificate Services	Builtin Object Token
Secure Certificate Services	Builtin Object Token
Trusted Certificate Services	Builtin Object Token
COMODO ECC Domain Validation Secure Server CA 2	Software Security Device
COMODO RSA Domain Validation Secure Server CA	Software Security Device
COMODO High Assurance Secure Server CA	Software Security Device
▼ ComSign	
ComSign CA	Builtin Object Token
ComSign Secured CA	Builtin Object Token
▼ Cybertrust, Inc	
Cybertrust Global Root	Builtin Object Token
▼ D-Trust GmbH	
D-TRUST Root Class 3 CA 2 EV 2009	Builtin Object Token
D-TRUST Root Class 3 CA 2 2009	Builtin Object Token
▼ Dell Inc.	
iDRAC6 default certificate	Software Security Device
▼ Deutsche Telekom AG	
Deutsche Telekom Root CA 2	Builtin Object Token
▼ Deutscher Sparkassen Verlag GmbH	
S-TRUST Authentication and Encryption Root CA 2005:PN	Builtin Object Token
S-TRUST Universal Root CA	Builtin Object Token
▼ Dhimyotis	
Certigna	Builtin Object Token
▼ DigiCert Inc	
DigiCert Trusted Root G4	Builtin Object Token
DigiCert Global Root CA	Builtin Object Token
DigiCert Assured ID Root G3	Builtin Object Token

Local Trust

That's a big list of people to Trust

Are they all trustable?

Evidently Not!



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
certSIGN ROOT CA	Builtin Object Token
China Financial Certification Authority	
CFCA EV ROOT	Builtin Object Token
China Internet Network Information Center	
China Internet Network Information Center EV Certificates Root	Builtin Object Token
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 D	
COMODO RSA D	
COMODO High	
ComSign	
ComSign CA	
ComSign Secure	
Cybertrust, Inc	
Cybertrust Glob	
D-Trust GmbH	
D-TRUST Root C	
D-TRUST Root C	
Dell Inc.	
iDRAC6 default	
Deutsche Telekom	
Deutsche Telek	
Deutscher Sparkass	
S-TRUST Authen	
S-TRUST Univer	
Dhimyotis	
Certigna	
DigiCert Inc	
DigiCert Truste	
DigiCert Global	
DigiCert Assure	

View...
Ed
googleonlinesecurity.blogspot.com.au/2015/03/mainta
Google Online Security Blog: Maintaining digital certificate security
G+1
106

Maintaining digital certificate security

Posted: Monday, March 23, 2015

Posted by Adam Langley, Security Engineer

On Friday, March 20th, we became aware of unauthorized digital certificates for several Google domains. The certificates were issued by an intermediate certificate authority apparently held by a company called MCS Holdings. This intermediate certificate was issued by CNNIC.

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.

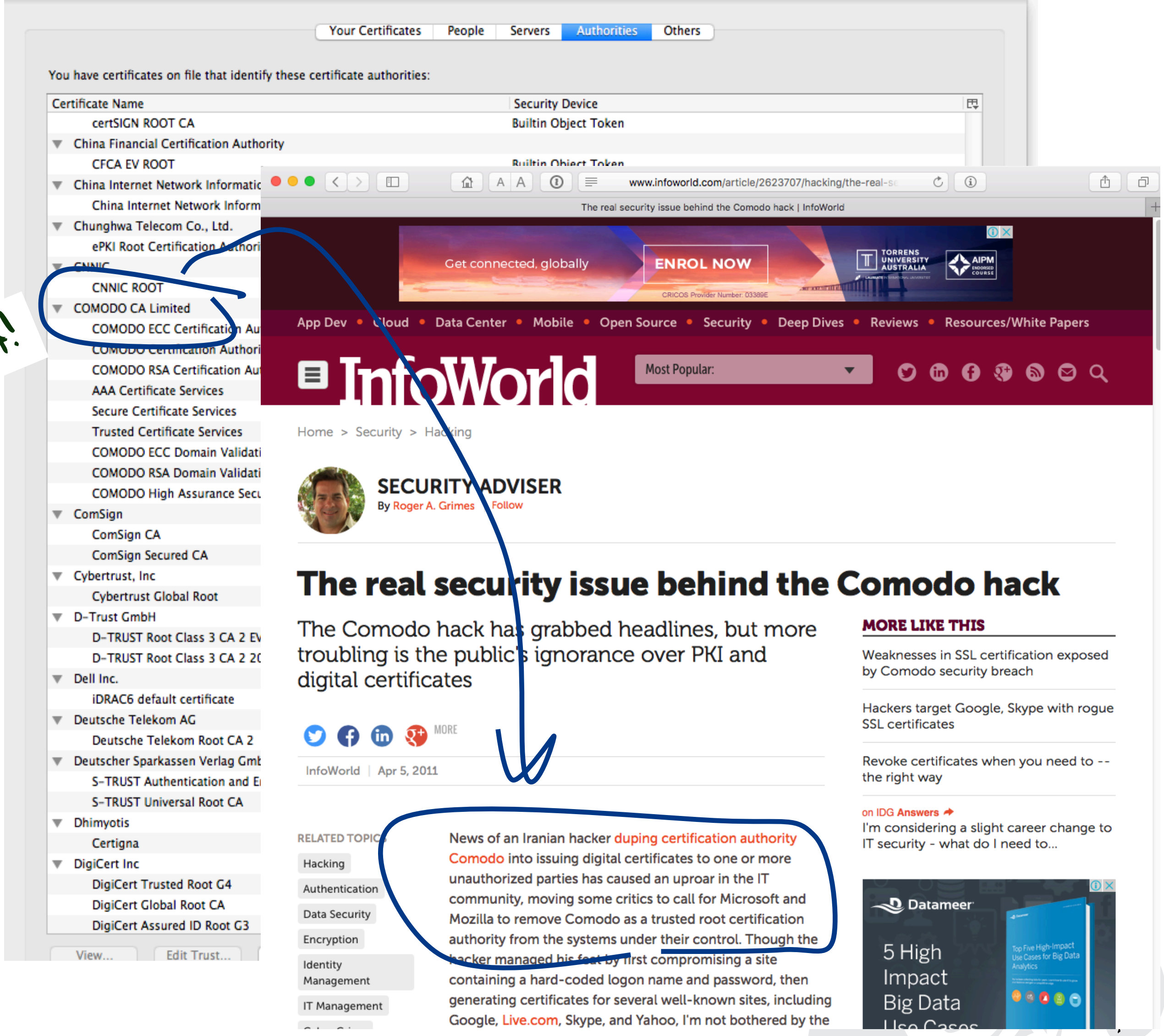
We promptly alerted CNNIC and other major browsers about the incident, and we blocked the MCS Holdings certificate in Chrome with a CRLSet push. CNNIC responded on the 22nd to explain that they had contracted with MCS Holdings on the basis that MCS would only issue certificates for domains that they 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 Trust

That’s a big list of people to Trust

Are they all trustable?

Evidently Not!



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
certSIGN ROOT CA	Builtin Object Token
▼ China Financial Certification Authority	
CFCA EV ROOT	Builtin Object Token
▼ China Internet Network Informatic	
China Internet Network Inform	
▼ Chunghwa Telecom Co., Ltd.	
ePKI Root Certification Authori	
▼ CNNIC	
CNNIC ROOT	
▼ COMODO CA Limited	
COMODO ECC Certification Au	
COMODO Certification Authori	
COMODO RSA Certification Au	
AAA Certificate Services	
Secure Certificate Services	
Trusted Certificate Services	
COMODO ECC Domain Validati	
COMODO RSA Domain Validati	
COMODO High Assurance Secu	
▼ ComSign	
ComSign CA	
ComSign Secured CA	
▼ Cybertrust, Inc	
Cybertrust Global Root	
▼ D-Trust GmbH	
D-TRUST Root Class 3 CA 2 EV	
D-TRUST Root Class 3 CA 2 20	
▼ Dell Inc.	
iDRAC6 default certificate	
▼ Deutsche Telekom AG	
Deutsche Telekom Root CA 2	
▼ Deutscher Sparkassen Verlag Gmb	
S-TRUST Authentication and E	
S-TRUST Universal Root CA	
▼ Dhimyotis	
Certigna	
▼ DigiCert Inc	
DigiCert Trusted Root G4	
DigiCert Global Root CA	
DigiCert Assured ID Root G3	

www.infoworld.com/article/2623707/hacking/the-real-se
The real security issue behind the Comodo hack | InfoWorld

App Dev • Cloud • Data Center • Mobile • Open Source • Security • Deep Dives • Reviews • Resources/White Papers
InfoWorld
Most Popular:

Home > Security > Hacking

SECURITY ADVISER
By Roger A. Grimes Follow

The real security issue behind the Comodo hack

The Comodo hack has grabbed headlines, but more troubling is the public's ignorance over PKI and digital certificates

InfoWorld | Apr 5, 2011

RELATED TOPICS

- Hacking
- Authentication
- Data Security
- Encryption
- Identity Management
- IT Management

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

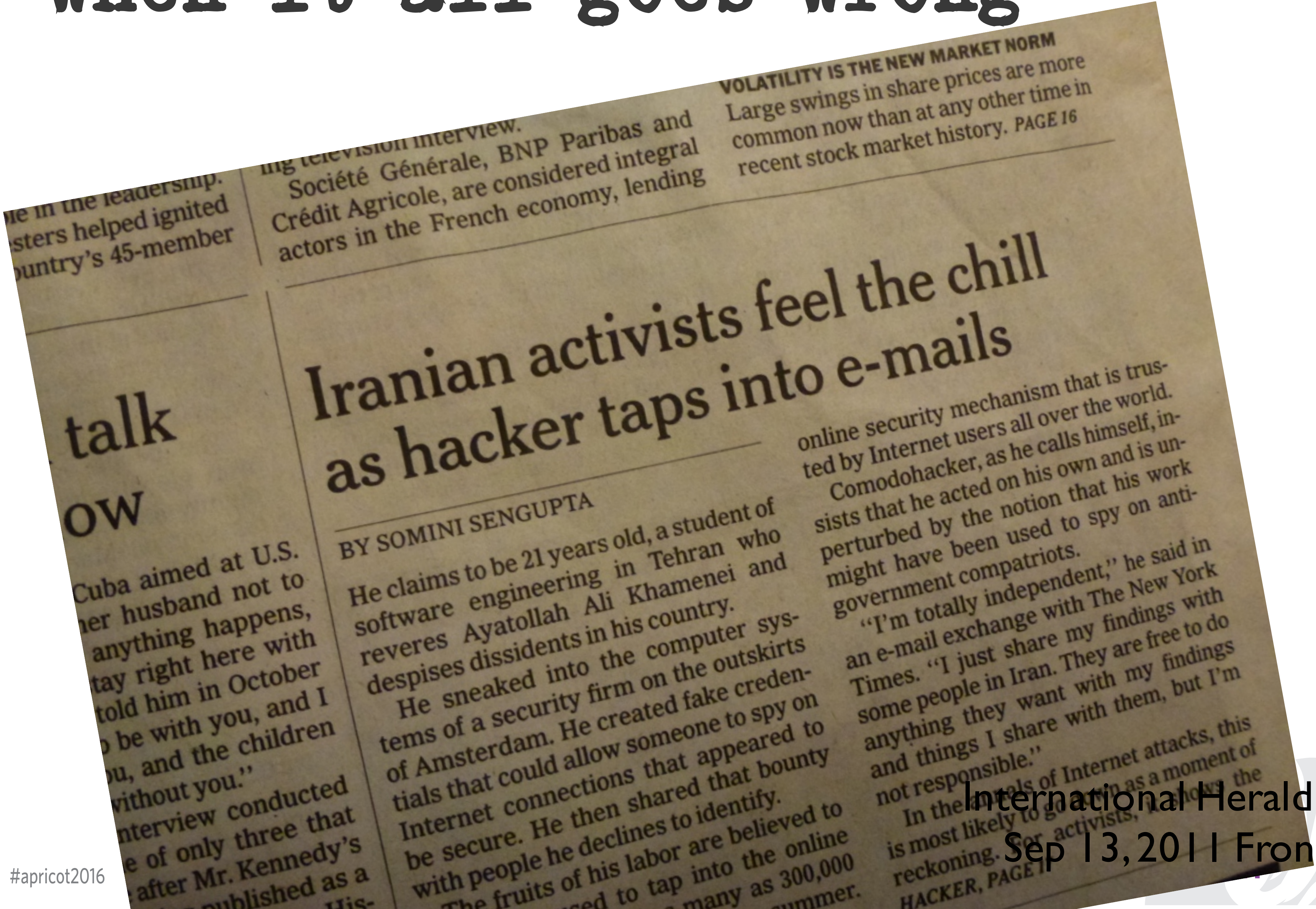
MORE LIKE THIS

- Weaknesses in SSL certification exposed by Comodo security breach
- Hackers target Google, Skype with rogue SSL certificates
- Revoke certificates when you need to -- the right way

on IDG Answers
I'm considering a slight career change to IT security - what do I need to...

With unpleasant consequences when it all goes wrong

With unpleasant consequences when it all goes wrong



...le in the leadership. ...sters helped ignited ...ountry'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*

... talk ... ow

...Cuba aimed at U.S. ...her husband not to ... anything happens, ...tay right here with ...told him in October ...o be with you, and I ...ou, and the children ...without you.'' ...nterview conducted ...e of only three that ... after Mr. Kennedy's ...published as a ...His-

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 ...sed to tap into the online ... many as 300,000 ...summer.

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.

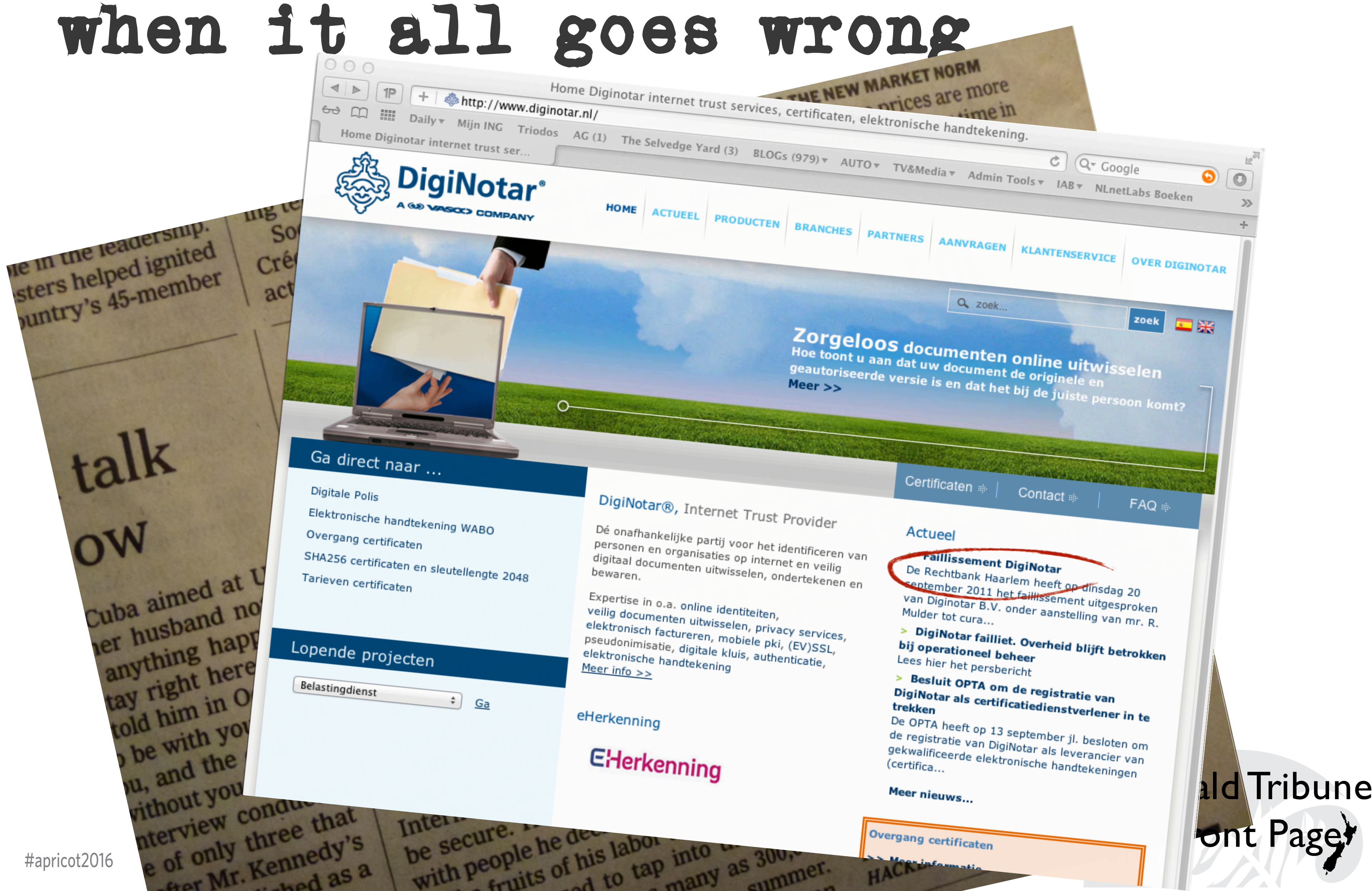
"I'm totally independent," he said in an e-mail exchange with The New York Times. "I just share my findings with some people in Iran. They are free to do anything they want with my findings and things I share with them, but I'm not responsible."

In the [illegible]als of Internet attacks, this is most likely to g[illegible] as a moment of reckoning. For activists, it shows the

HACKER, PAGE ...

International Herald Tribune
Sep 13, 2011 Front Page

With unpleasant consequences when it all goes wrong



Home Diginotar internet trust services, certificaten, elektronische handtekening.

http://www.diginotar.nl/

Zorgeloos documenten online uitwisselen
Hoe toont u aan dat uw document de originele en geautoriseerde versie is en dat het bij de juiste persoon komt?
Meer >>

Ga direct naar ...

- Digitale Polis
- Elektronische handtekening WABO
- Overgang certificaten
- SHA256 certificaten en sleutellengte 2048
- Tarieven certificaten

Lopende projecten

Belastingdienst ⬍ Ga

DigiNotar®, Internet Trust Provider

Dé onafhankelijke partij voor het identificeren van personen en organisaties op internet en veilig digitaal documenten uitwisselen, ondertekenen en bewaren.

Expertise in o.a. online identiteiten, veilig documenten uitwisselen, privacy services, elektronisch factureren, mobiele pki, (EV)SSL, pseudonimisatie, digitale kluis, authenticatie, elektronische handtekening
Meer info >>

eHerkenning

EHerkenning

Actueel

Faillissement DigiNotar
De Rechtbank Haarlem heeft op dinsdag 20 september 2011 het faillissement uitgesproken van Diginotar B.V. onder aanstelling van mr. R. Mulder tot cura...

> **DigiNotar failliet. Overheid blijft betrokken bij operationeel beheer**
Lees hier het persbericht

> **Besluit OPTA om de registratie van DigiNotar als certificatiedienstverlener in te trekken**
De OPTA heeft op 13 september jl. besloten om de registratie van DigiNotar als leverancier van gekwalificeerde elektronische handtekeningen (certifica...

Meer nieuws...

Overgang certificaten
>> Meer informatie

ald Tribune
ont Page

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 the digital certific
- You ANY CA to be used to validate a cert icate

WOW! That's awesomely bad!

What's going wrong here?

- The TLS handshake cannot specify WHICH CA should be used to validate the digital certifi
- You ANY CA to be used to validate a cert

WOW! That's awesomely bad!

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!

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?

Sustai..able
Resilient
Secure
Privacy
Trusted

?

In a commercial environment

Where CA's compete with each other for market share

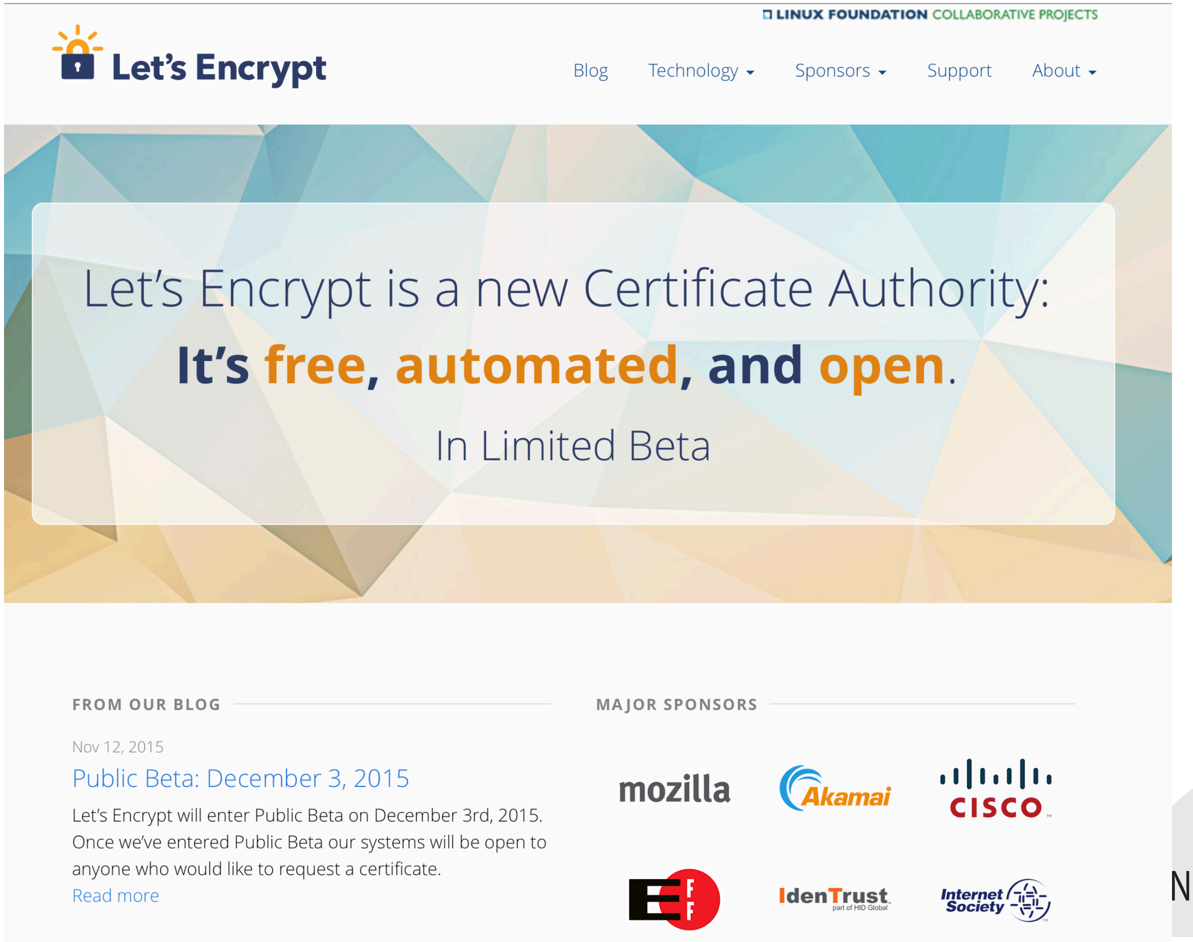
And quality offers no protection

Than what 'wins' in the market?

Sustainable
Resilient
Secure
Privacy
Trusted
Cheap!

Where now?

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



Let's Encrypt is a new Certificate Authority:

It's free, automated, and open.

In Limited Beta

FROM OUR BLOG

Nov 12, 2015

Public Beta: December 3, 2015

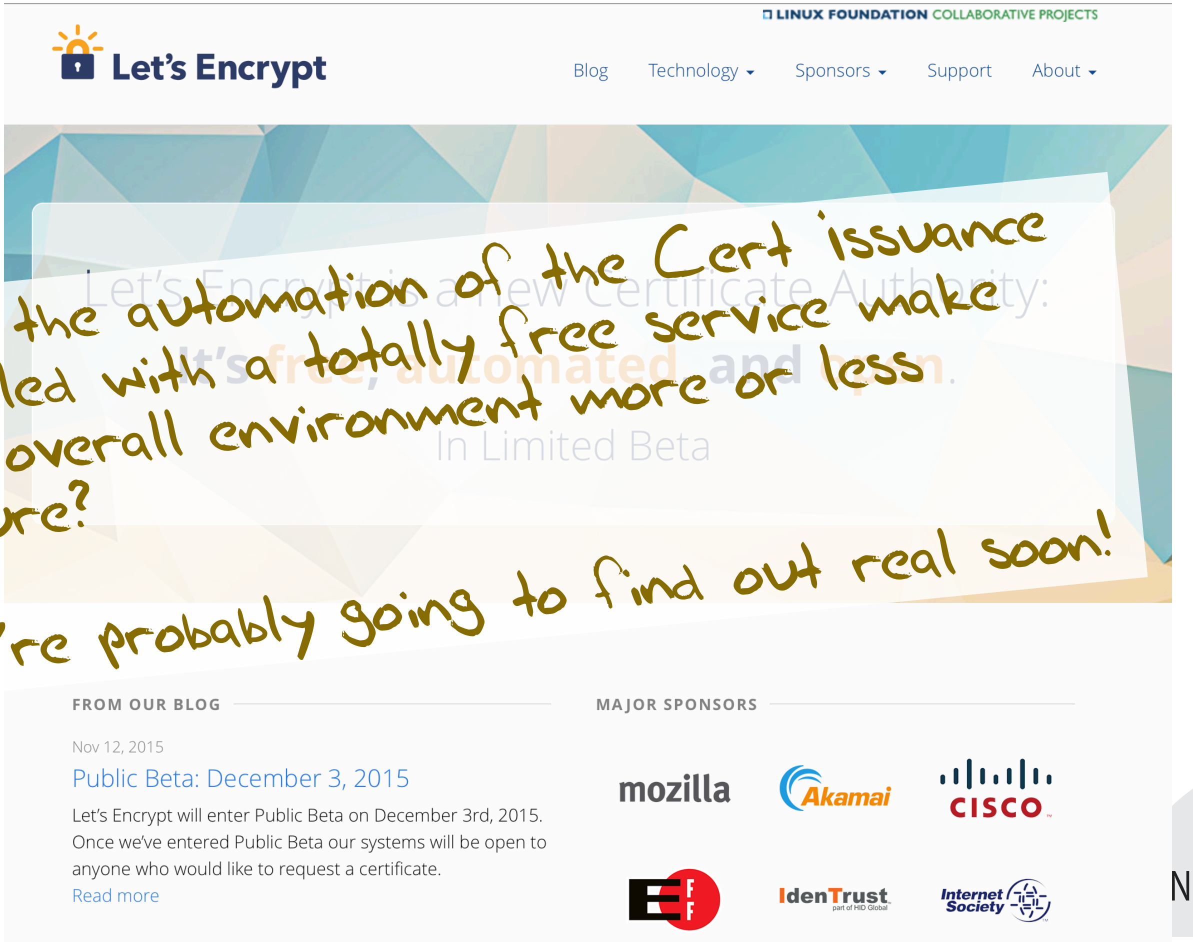
Let's Encrypt will enter Public Beta on December 3rd, 2015. Once we've entered Public Beta our systems will be open to anyone who would like to request a certificate.

Read more

MAJOR SPONSORS

Where now?

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



Let's Encrypt is a new Certificate Authority:

It's a free, automated, and open.

In Limited Beta

FROM OUR BLOG

Nov 12, 2015

Public Beta: December 3, 2015

Let's Encrypt will enter Public Beta on December 3rd, 2015. Once we've entered Public Beta our systems will be open to anyone who would like to request a certificate.

Read more

MAJOR SPONSORS

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?

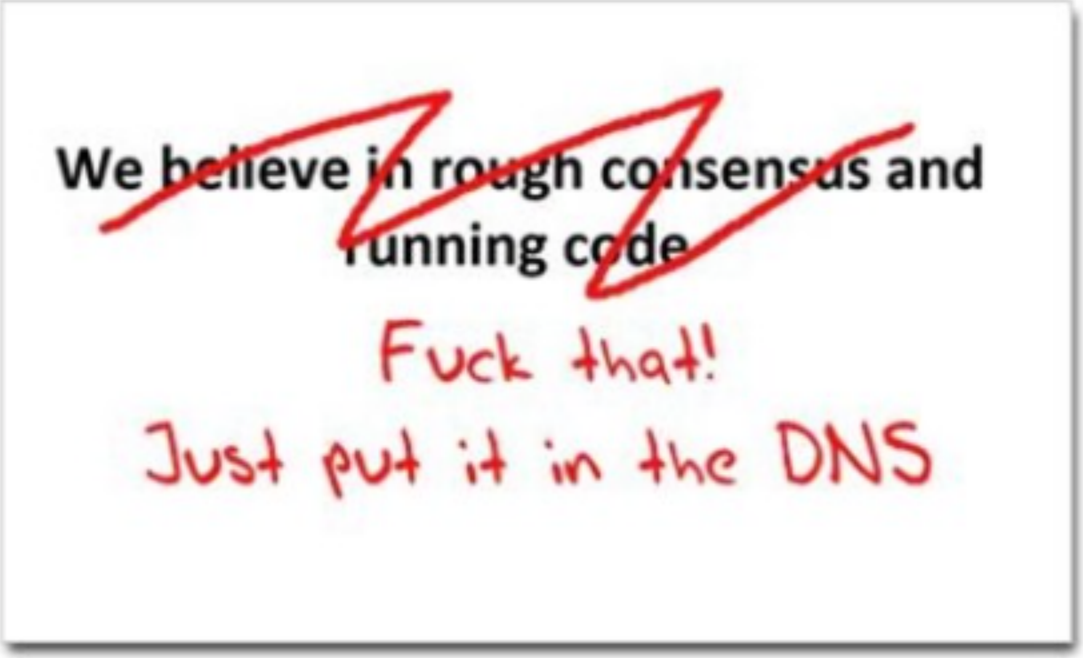
Option B: White Listing and Pinning with HSTS

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!



~~We believe in rough consensus and running code~~

Fuck that!

Just put it in the DNS

cafepress.com/nxdomain

Seriously

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

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 domain name public key cert as a simple self-signed cert?

Seriously

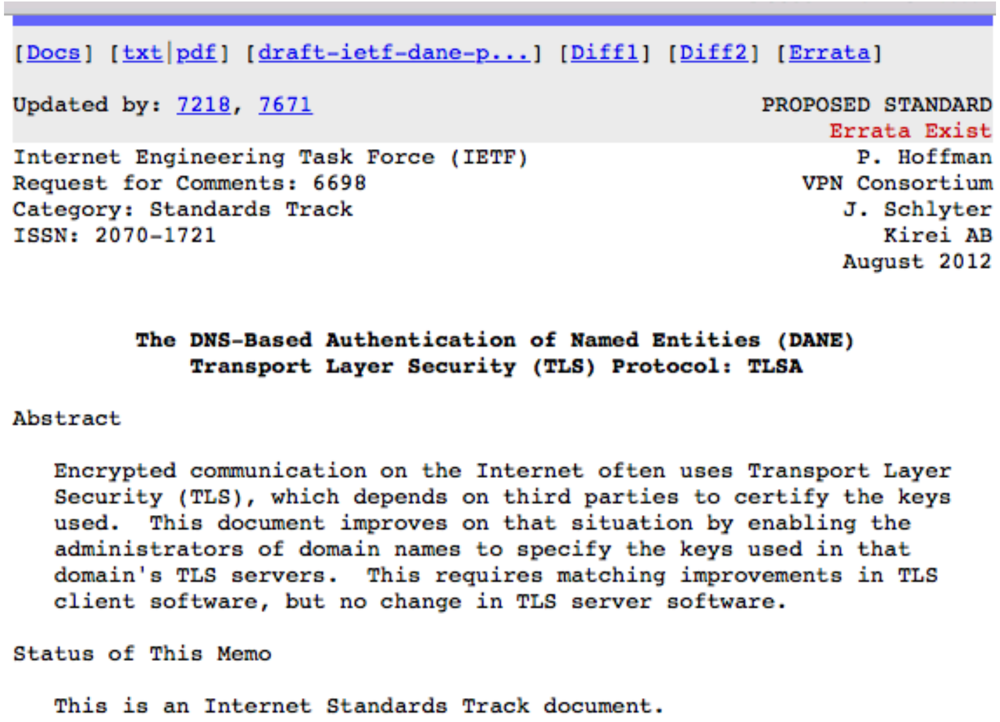
Where better to find out the public key as[illegible]ciated with a DNS name than to look it up in the DNS[illegible]

- Why not query the DNS for th[illegible]ord?
- Why not query the DN[illegible]suer CA?
- Why not quer[illegible] the hash of the domain name cert?
- Why n[illegible] DNS for the domain name public key cert as a si[illegible]signed cert?

Who needs CA's anyway?

DANE

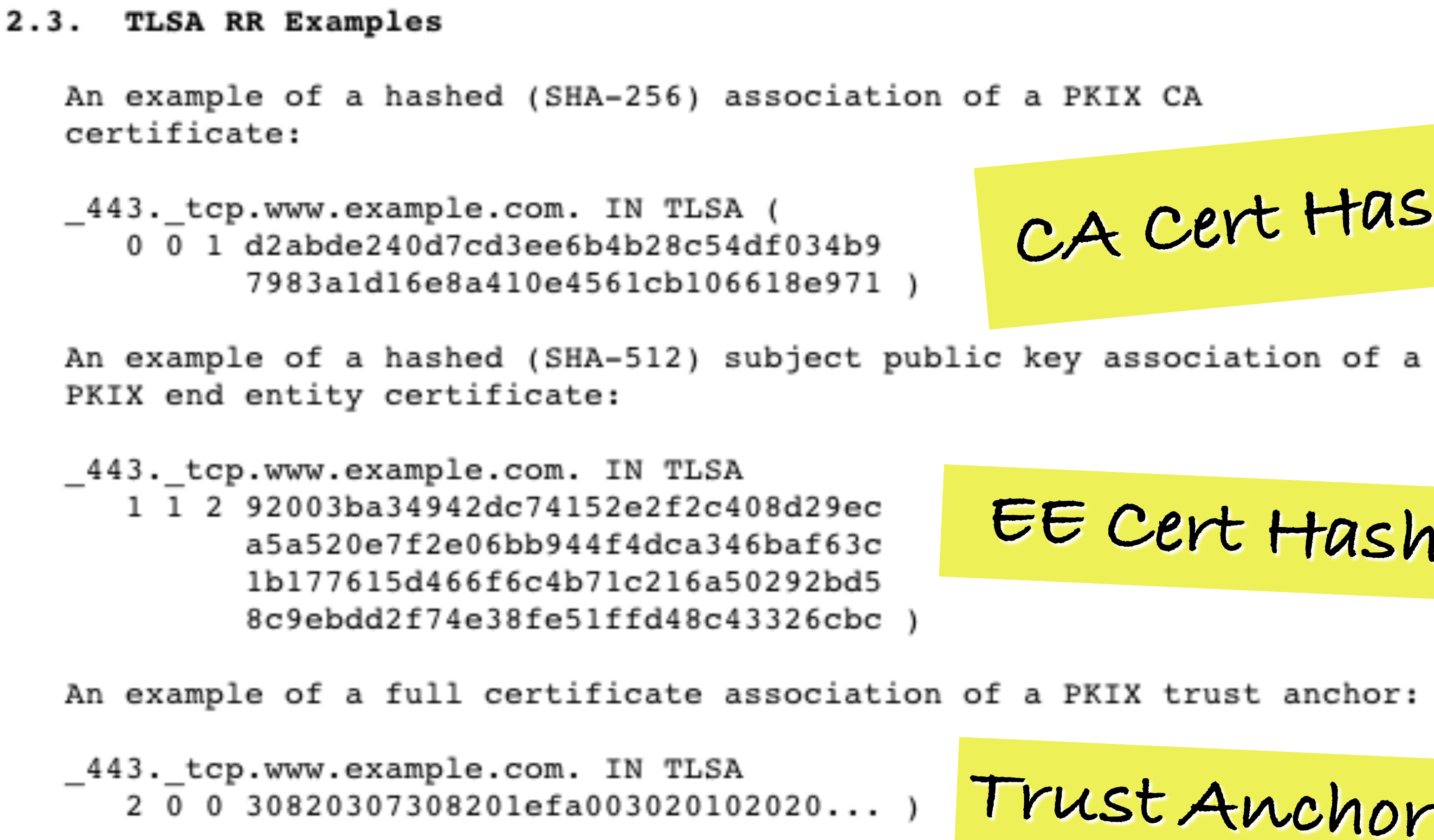
- Using the DNS to associated domain name public key certificates with domain name



```
[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
Request for Comments: 6698                            VPN Consortium
Category: Standards Track                                J. Schlyter
ISSN: 2070-1721                                             Kirei AB
                                                         August 2012


         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

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:

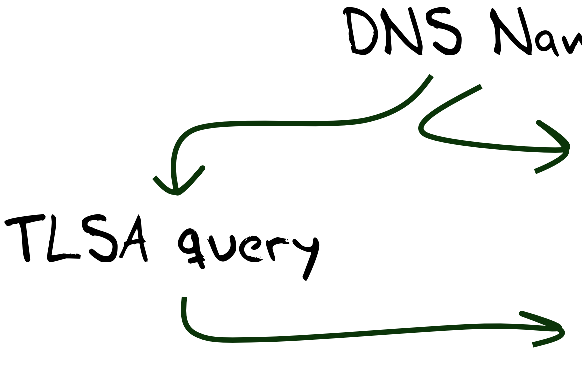
```
_443._tcp.www.example.com. IN TLSA
   2 0 0 30820307308201efa003020102020... )
```

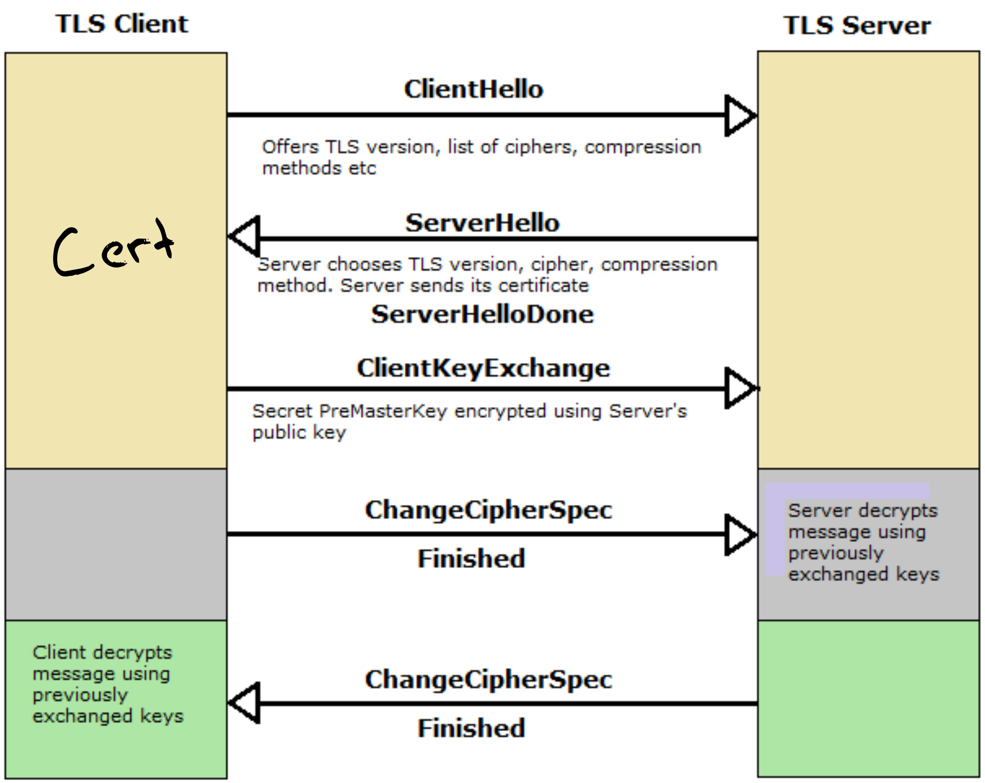
Trust Anchor

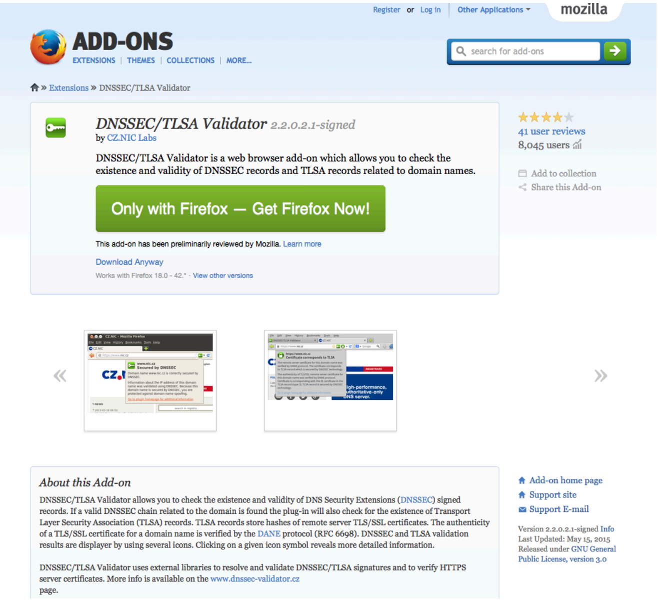
TLS with DANE

- 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




TLS Client
TLS Server
Cert
ClientHello
Offers TLS version, list of ciphers, compression methods etc
ServerHello
Server chooses TLS version, cipher, compression method. Server sends its certificate
ServerHelloDone
ClientKeyExchange
Secret PreMasterKey encrypted using Server's public key
ChangeCipherSpec
Finished
Server decrypts message using previously exchanged keys
Client decrypts message using previously exchanged keys
ChangeCipherSpec
Finished


Register or Log in | Other Applications ▾ mozilla
ADD-ONS
EXTENSIONS | THEMES | COLLECTIONS | MORE...
search for add-ons
» Extensions » DNSSEC/TLSA Validator

DNSSEC/TLSA Validator *2.2.0.2.1-signed*
by CZ.NIC Labs

DNSSEC/TLSA Validator is a web browser add-on which allows you to check the existence and validity of DNSSEC records and TLSA records related to domain names.

Only with Firefox — Get Firefox Now!

This add-on has been preliminarily reviewed by Mozilla. Learn more

Download Anyway

Works with Firefox 18.0 - 42.* · View other versions

★★★★☆
41 user reviews
8,045 users

Add to collection
Share this Add-on
«
»

About this Add-on

DNSSEC/TLSA Validator allows you to check the existence and validity of DNS Security Extensions (DNSSEC) signed records. If a valid DNSSEC chain related to the domain is found the plug-in will also check for the existence of Transport Layer Security Association (TLSA) records. TLSA records store hashes of remote server TLS/SSL certificates. The authenticity of a TLS/SSL certificate for a domain name is verified by the DANE protocol (RFC 6698). DNSSEC and TLSA validation results are displayer by using several icons. Clicking on a given icon symbol reveals more detailed information.

DNSSEC/TLSA Validator uses external libraries to resolve and validate DNSSEC/TLSA signatures and to verify HTTPS server certificates. More info is available on the www.dnssec-validator.cz page.

Version 2.2.0.2.1-signed Info
Last Updated: May 15, 2015
Released under GNU General Public License, version 3.0

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

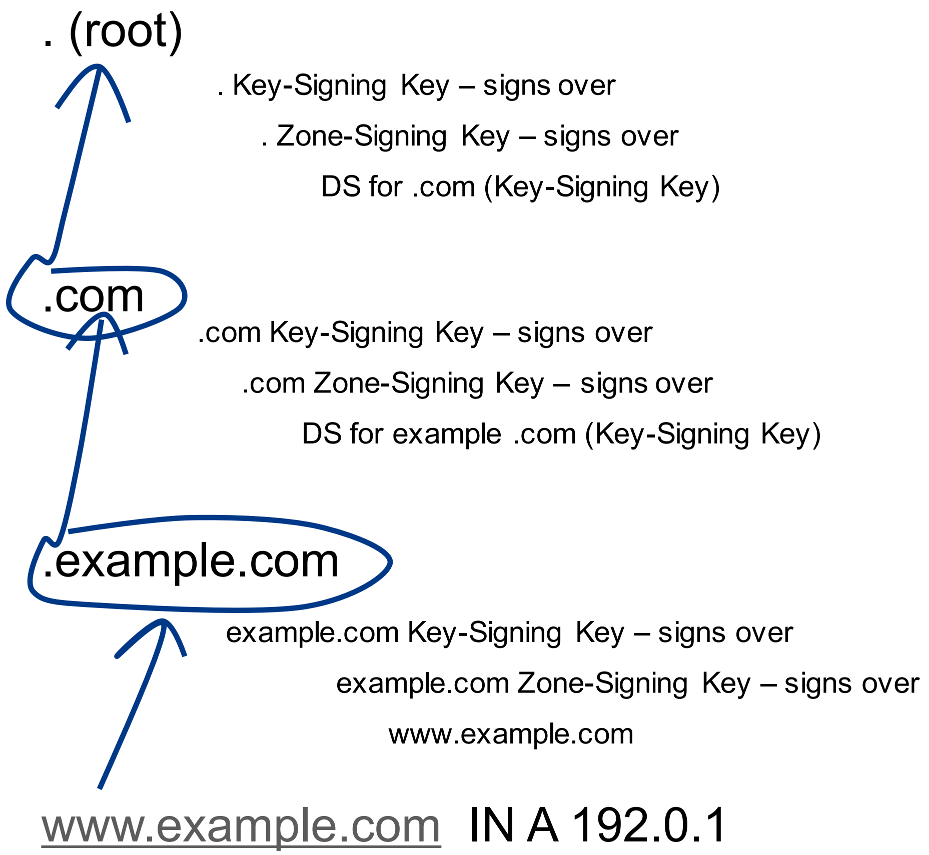
example.com Key-Signing Key – signs over

example.com Zone-Signing Key – signs over

www.example.com

www.example.com

DNSSEC Interlocking Signatures



. (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

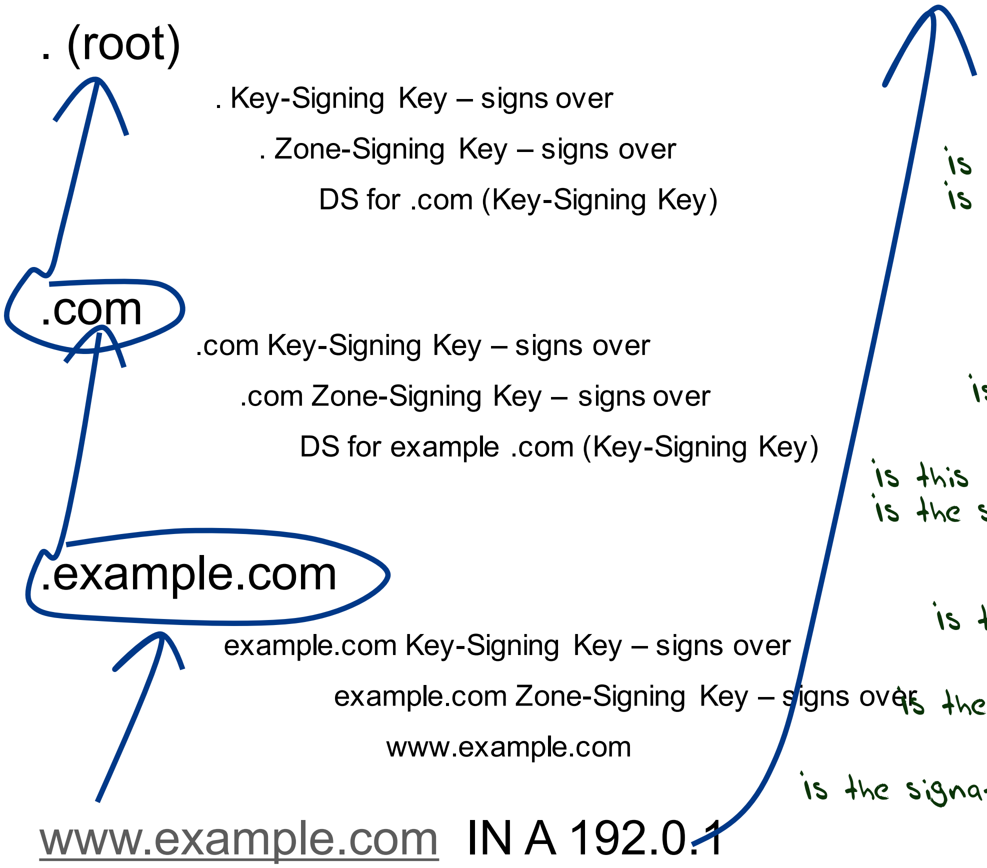
example.com Key-Signing Key – signs over

example.com Zone-Signing Key – signs over

www.example.com

www.example.com IN A 192.0.1

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 IN A 192.0.1

is the KSK for . valid?

is the ZSK for . valid?

is this DS equal to the hash of the KSK?
is the signature for this record valid?

is the KSK for .com valid?

is the ZSK for .com valid?

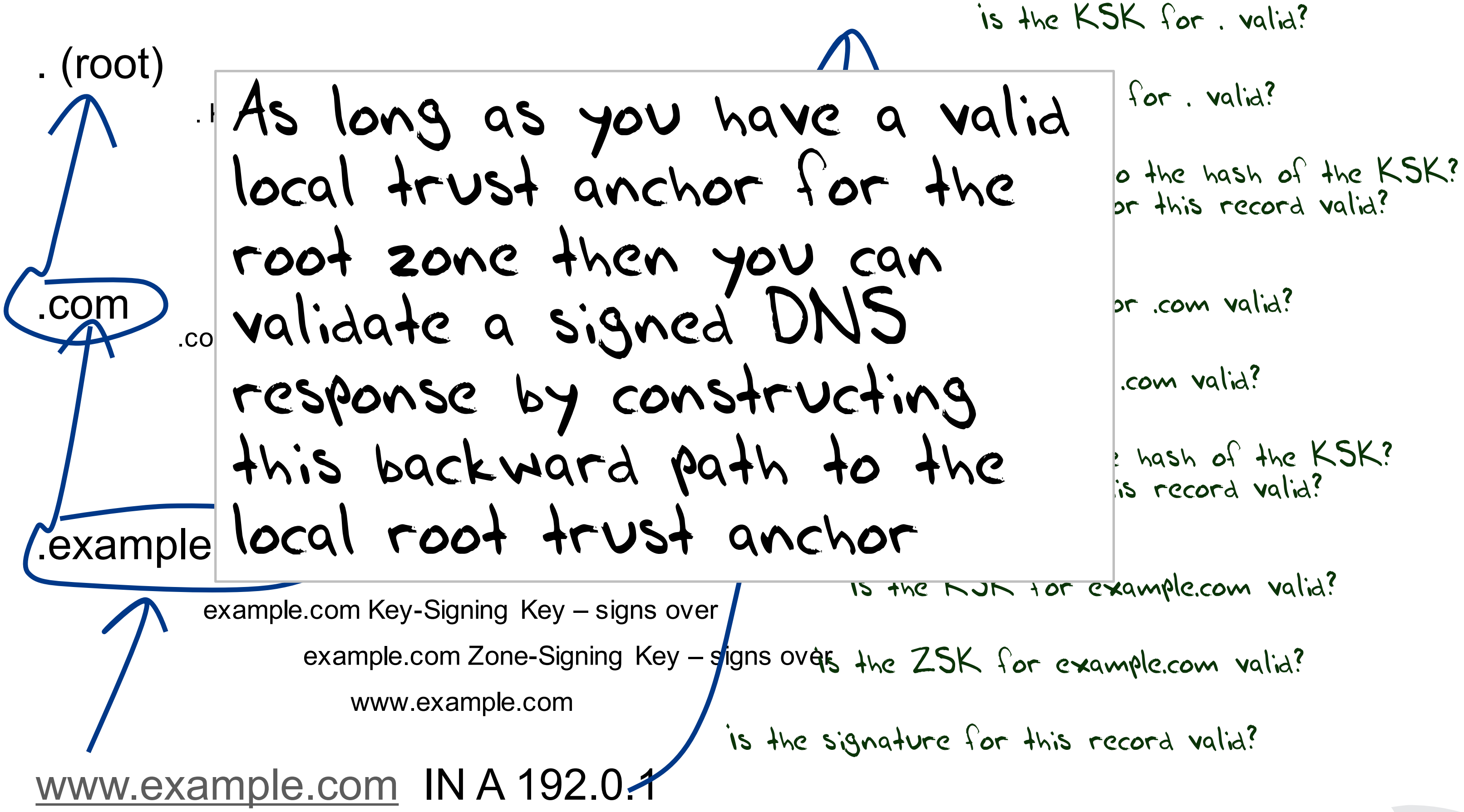
is this DS equal to the hash of the KSK?
is the signature for this record valid?

is the KSK for example.com valid?

is the ZSK for example.com valid?

is the signature for this record valid?

DNSSEC Interlocking Signatures



. (root)

.com

.co

.example

example.com Key-Signing Key – signs over

example.com Zone-Signing Key – signs over

www.example.com

www.example.com IN A 192.0.1

is the KSK for . valid?

for . valid?

o the hash of the KSK?
or this record valid?

or .com valid?

.com valid?

hash of the KSK?
is record valid?

is the KSK for example.com valid?

is the ZSK for example.com valid?

is the signature for this record valid?

As long as you have a valid local trust anchor for the root zone then you can validate a signed DNS response by constructing this backward path to the local root trust anchor

DANE + DNSSEC

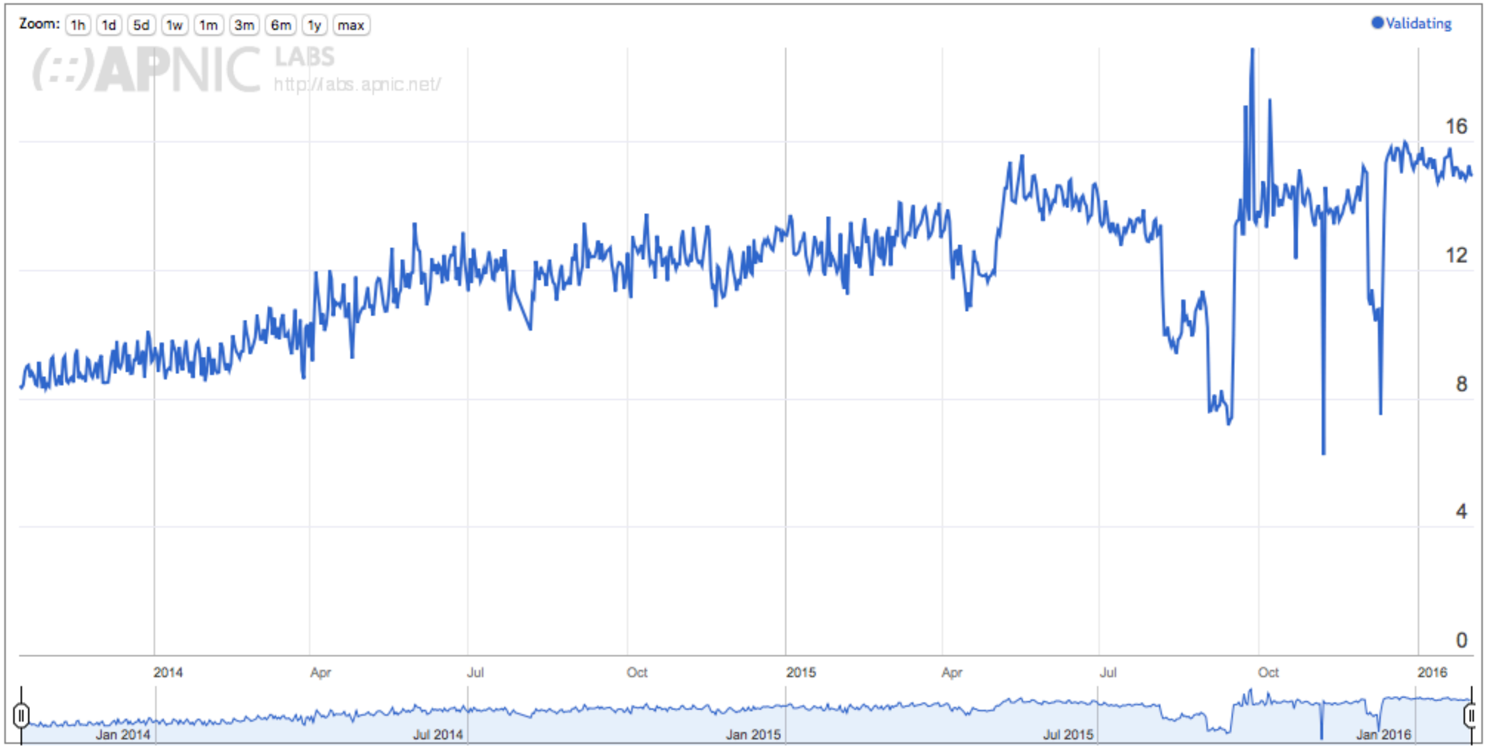
- Query the DNS for the TLSA record of the domain name and ask for the DNSSEC signature to be included in the response
- Validate the signature to ensure that you have an unbroken signature chain to the root trust point
- At this point you can accept the TLSA record as the authentic record, and set up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

Use of DNSSEC Validation for World (XA)



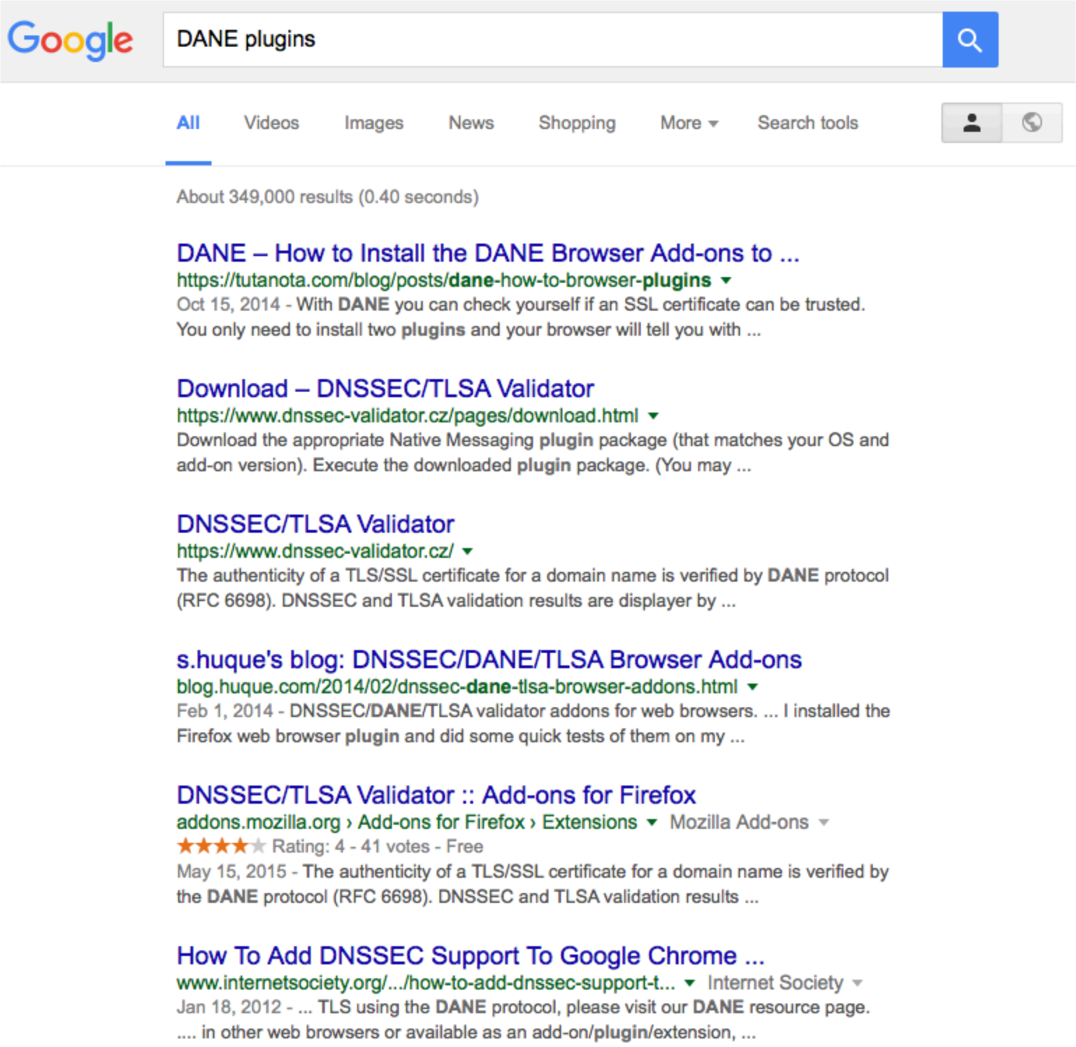
stats.labs.apnic.net/dnssec/XA

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?



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 displayer 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... ▾ Internet Society ▾
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!

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

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

That's it!

Questions?