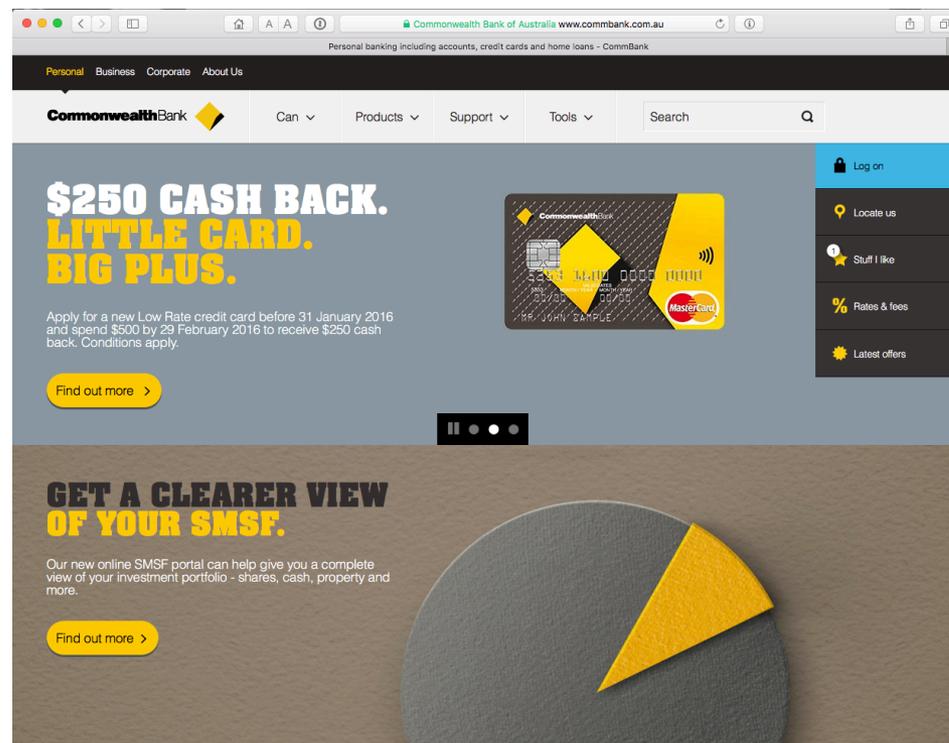


Why Dane?

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?



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.
```

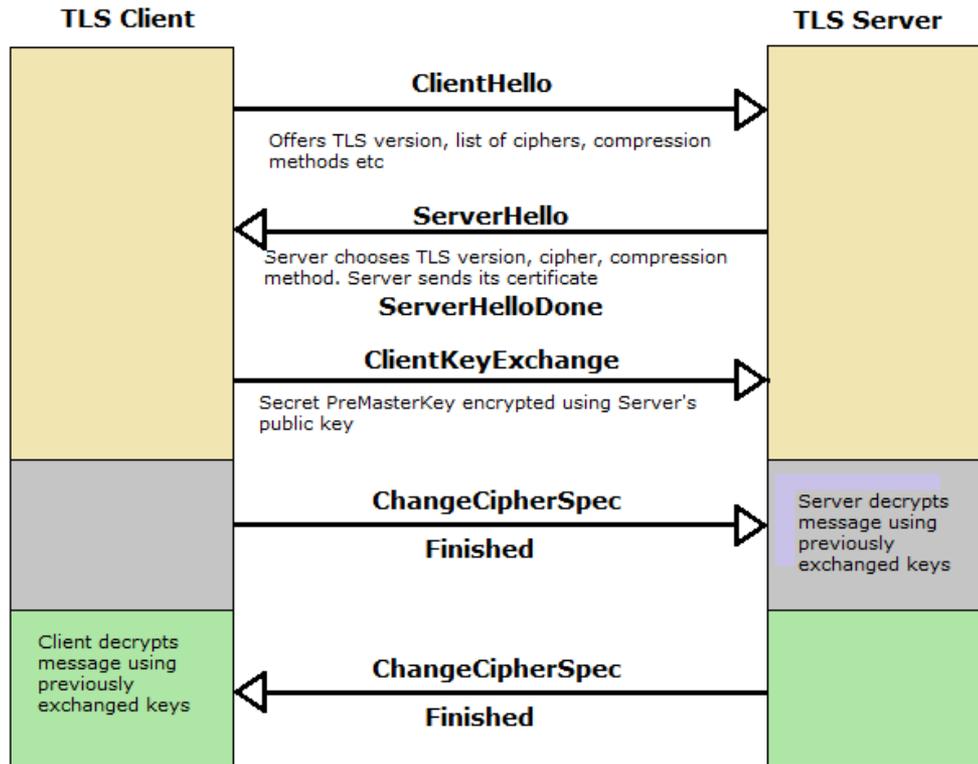
That's not an IP addresses that was allocated to the Commonwealth Bank!

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

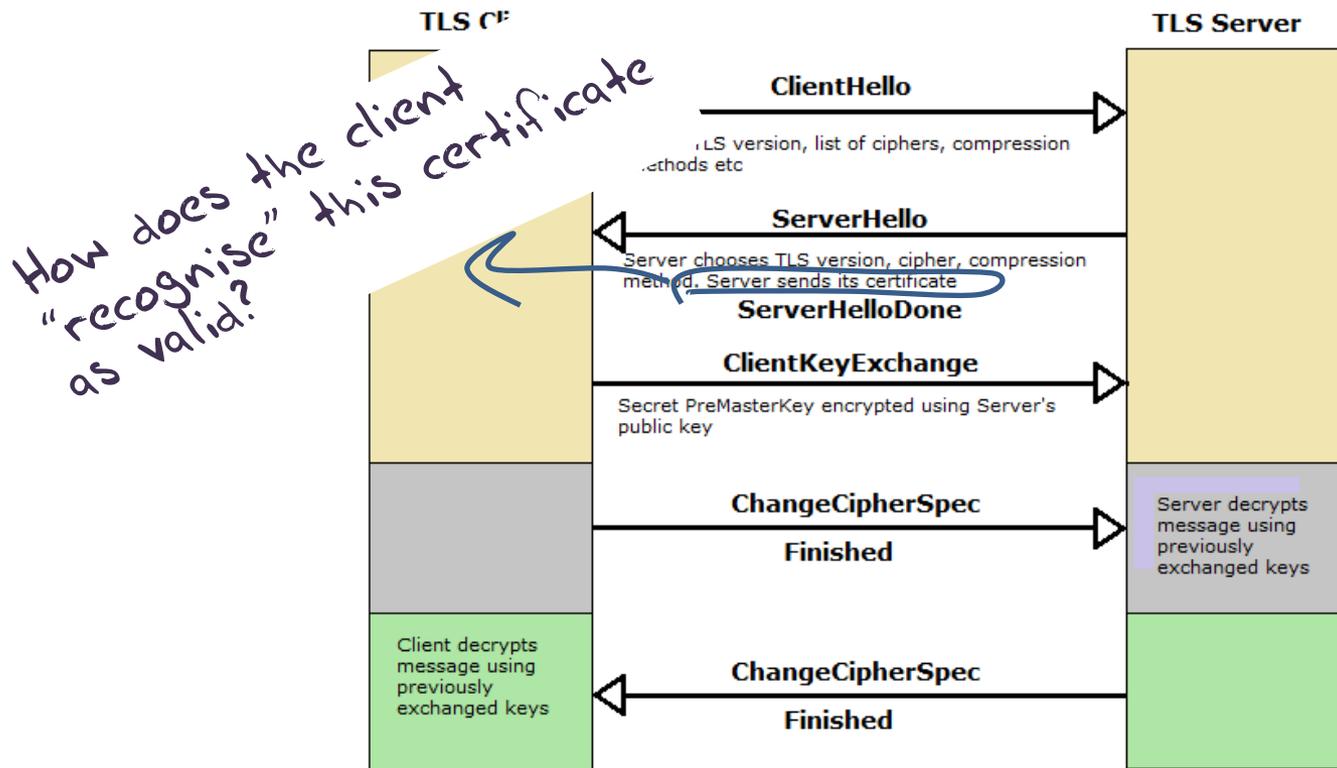
So why should my browser trust that 104.97.235.12 is really the “proper” web site for the Commonwealth Bank of Australia and not some dastardly evil scam?

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

TLS Connections



TLS Connections





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

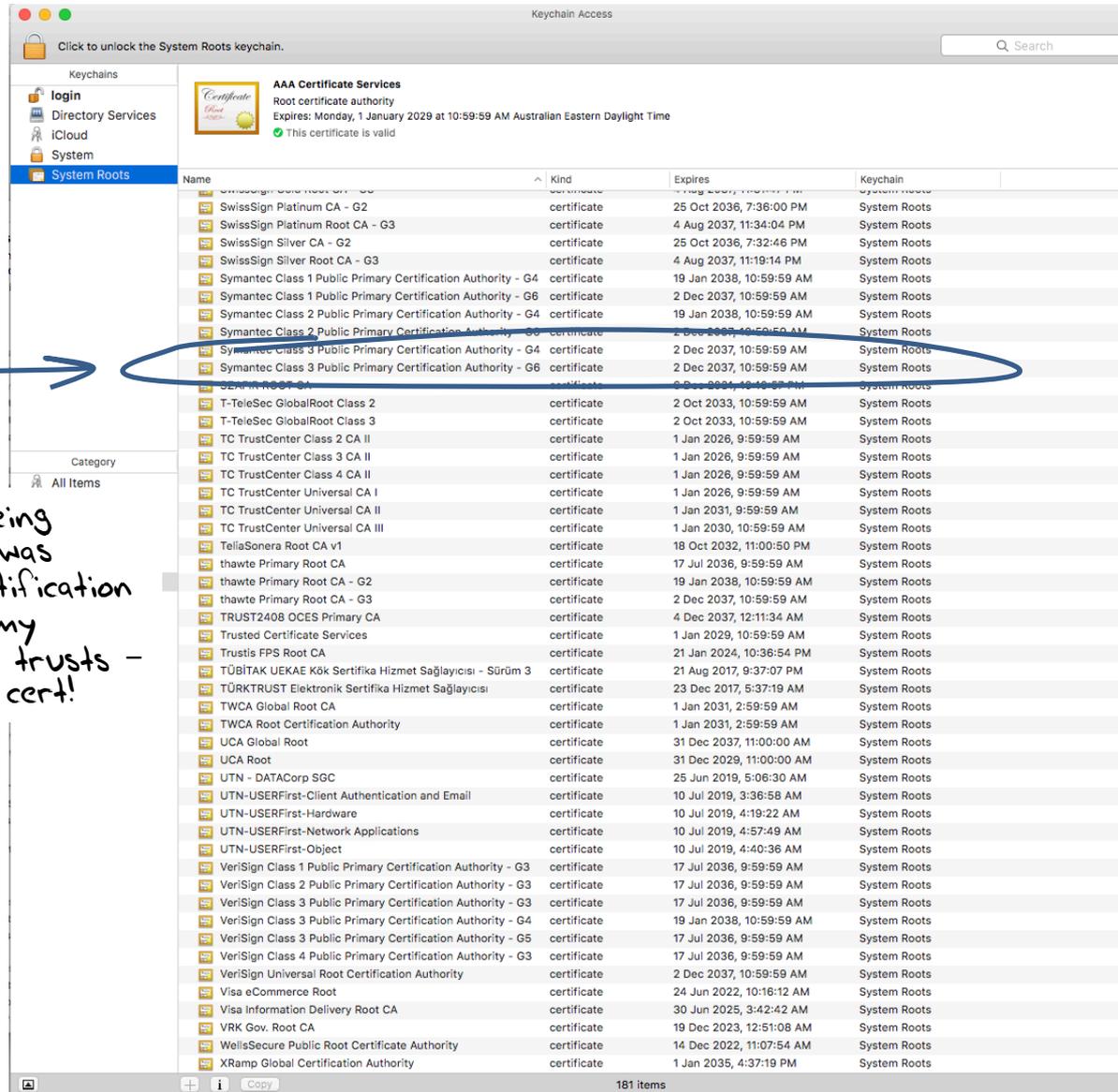
- The Commonwealth Bank of Australia has generated a key pair
- And they passed a certificate signing request to a company called “Symantec”
- Who is willing to vouch (in a certificate) that the entity who goes by the domain name of www.commbank.com.au also has a certain public key value
- So if I can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

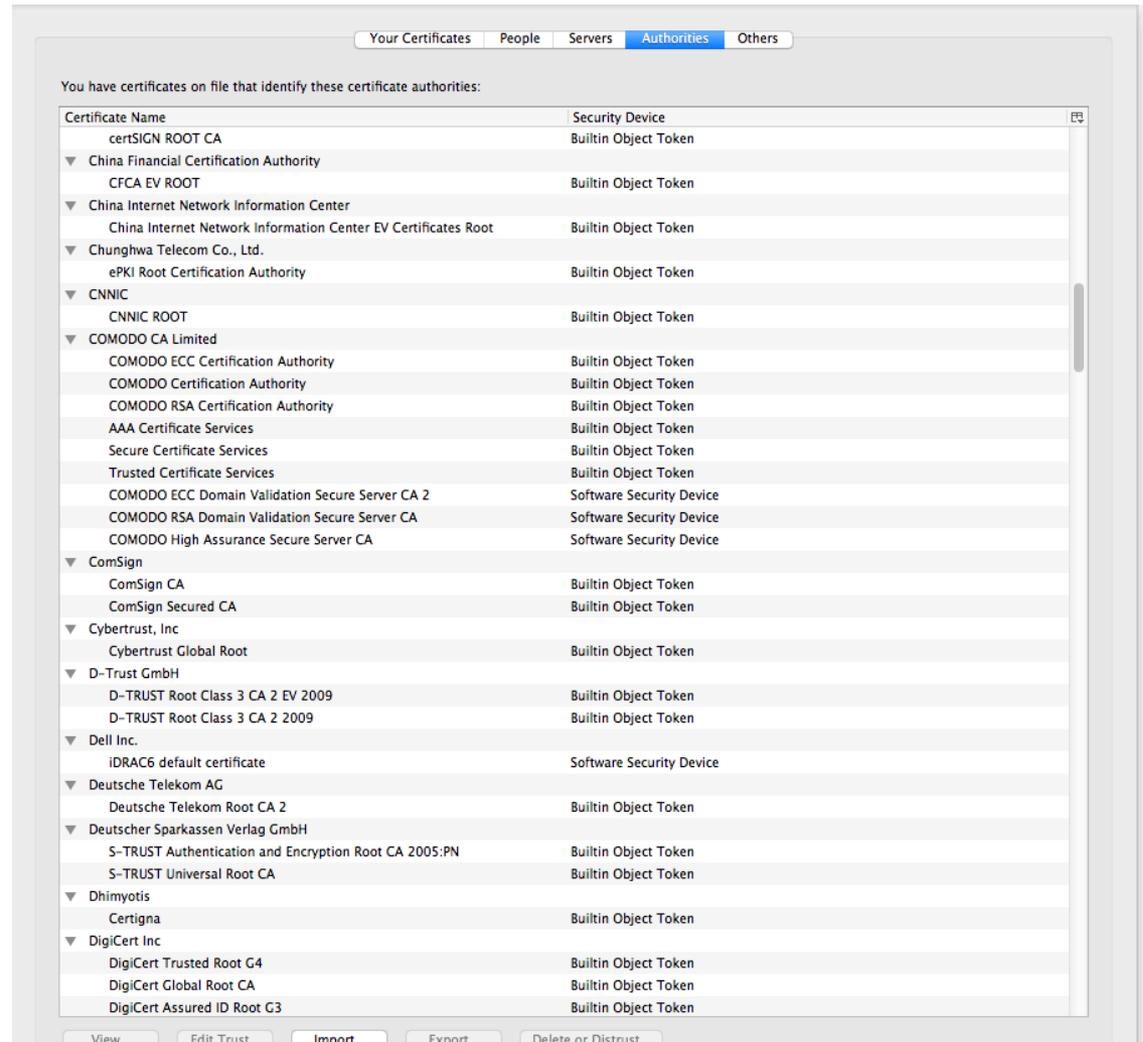


The cert I'm being asked to trust was issued by a certification authority that my browser already trusts - so I trust that cert!

Local Trust

That's a big list of people to Trust

Are they all trustable?



Local Trust

That's a big list of people to Trust

Are they all trustable?

Evidently Not!

Your Certificates | People | Servers | **Authorities** | Others

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
▼ Chungghwa 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 Securm	
▼ 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	
▼ Dhimiyotis	
Certigna	
▼ DigiCert Inc	
DigiCert Truste	
DigiCert Global	
DigiCert Assure	

View... Ed

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!

The screenshot shows the Windows Certificate Manager interface. The 'Authorities' tab is selected, displaying a list of certificate authorities. The entry 'COMODO CA Limited' is circled in blue. An arrow points from this circle to a browser window displaying an article titled 'The real security issue behind the Comodo hack' by Roger A. Grimes. A second blue circle highlights a paragraph in the article that reads: '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'.

With unpleasant consequences
when it all goes wrong

With unpleasant consequences when it all goes wrong

... in the leadership.
... sters helped ignited
... untry'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

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."

... interview conducted
... e of only three that
... after Mr. Kennedy's
... ublished 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 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
... many as 300,000
... 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 annals of Internet attacks, this
is most likely to go down as a moment of
reckoning. For activists, it shows the
HACKER, PAGE 11

With unpleasant consequences when it all goes wrong

The image shows a screenshot of the DigiNotar website in a web browser. The browser's address bar shows the URL <http://www.diginotar.nl/>. The website header includes the DigiNotar logo, the tagline "A GIGASOC COMPANY", and a navigation menu with items like HOME, ACTUEEL, PRODUCTEN, BRANCHES, PARTNERS, AANVRAGEN, KLANTENSERVICE, and OVER DIGINOTAR. A search bar is visible with the text "zoek...". The main banner features a hand holding a folder over a laptop, with the headline "Zorgeloos documenten online uitwisselen" and a sub-headline "Hoe toont u aan dat uw document de originele en geautoriseerde versie is en dat het bij de juiste persoon komt?". Below the banner, there are several sections: "Ga direct naar ..." with links for "Digitale Polis", "Elektronische handtekening WABO", "Overgang certificaten", "SHA256 certificaten en sleutellengte 2048", and "Tarieven certificaten"; "Lopende projecten" with a dropdown menu showing "Belastingdienst"; "DigiNotar®, Internet Trust Provider" with a paragraph describing their services and a link to "Meer info >>"; "Actueel" with a red circle around the heading "Faillissement DigiNotar" and a paragraph about a bankruptcy ruling by the Rechtbank Haarlem on September 20, 2011, and two sub-articles: "DigiNotar failliet. Overheid blijft betrokken bij operationeel beheer" and "Besluit OPTA om de registratie van DigiNotar als certificatieinstantie te trekken"; and "eHerkenning" with the logo "EHerkenning". At the bottom, there is a section for "Overgang certificaten" with a link to "Meer informatie".

Home Diginotar internet trust services, certificaten, elektronische handtekening.

Home Diginotar internet trust ser... AG (1) The Selvedge Yard (3) BLOGs (979) AUTO TV&Media Admin Tools IAB NLnetLabs Boeken

DigiNotar®
A GIGASOC COMPANY

HOME ACTUEEL PRODUCTEN BRANCHES PARTNERS AANVRAGEN KLANTENSERVICE OVER DIGINOTAR

zoek... zoek

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 certificatieinstantie 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

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 +
c) *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 sun icon with a padlock inside, followed by the text "Let's Encrypt". To the right of the logo is the text "LINUX FOUNDATION COLLABORATIVE PROJECTS". Below this is a navigation menu with links for "Blog", "Technology", "Sponsors", "Support", and "About". The main content area features a large, semi-transparent white box with a geometric, low-poly background. Inside this box, the text reads: "Let's Encrypt is a new Certificate Authority: **It's free, automated, and open.** In Limited Beta". Below the main content area, there are two columns of content. The left column is titled "FROM OUR BLOG" and contains a post dated "Nov 12, 2015" with the title "Public Beta: December 3, 2015". The text of the post states: "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." and includes a "Read more" link. The right column is titled "MAJOR SPONSORS" and features logos for "mozilla", "Akamai", "CISCO", "IdenTrust", and "Internet Society".

Let's Encrypt LINUX FOUNDATION COLLABORATIVE PROJECTS

Blog Technology Sponsors Support About

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

mozilla Akamai CISCO IdenTrust Internet Society

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, the Let's Encrypt logo is on the left, and the text "LINUX FOUNDATION COLLABORATIVE PROJECTS" is on the right. Below the logo is a navigation menu with links for "Blog", "Technology", "Sponsors", "Support", and "About". The main content area features a large banner with a geometric pattern. Overlaid on this banner is a white box containing handwritten text in brown ink: "Will the automation of the Cert issuance coupled with a totally free service make the overall environment more or less secure?". Below this box is another white box with the text "We're probably going to find out real soon!". The banner also contains the text "Let's Encrypt is a new Certificate Authority: It's free, automated and open. In Limited Beta". At the bottom of the page, there are two sections: "FROM OUR BLOG" and "MAJOR SPONSORS". The "FROM OUR BLOG" section has a date "Nov 12, 2015" and a title "Public Beta: December 3, 2015", followed by a short paragraph and a "Read more" link. The "MAJOR SPONSORS" section lists logos for mozilla, Akamai, CISCO, E F, IdenTrust, and Internet Society.

Let's Encrypt is a new Certificate Authority: It's free, automated and open. In Limited Beta

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!

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

mozilla Akamai CISCO E F IdenTrust Internet Society

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

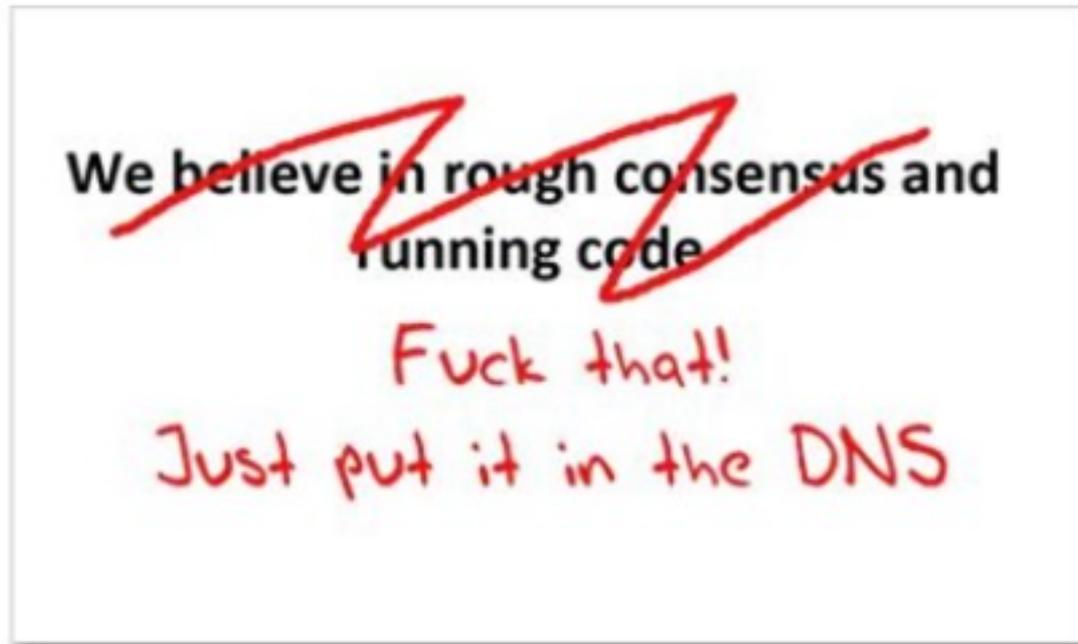
Where now?

Option B: White Listing and Pinning with HSTS

https://code.google.com/p/chromium/src/trunk/net/http_transport_security_state_static.json *its not a totally insane idea -- until you realise that it appears to be completely unscalable!*

Where now?

Option C: Use the DNS!



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 associated with a DNS record to look it up in the DNS?

– Why not query the DNS for the HSTS record?

– *Who needs CA's anyway?* 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?

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  
      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

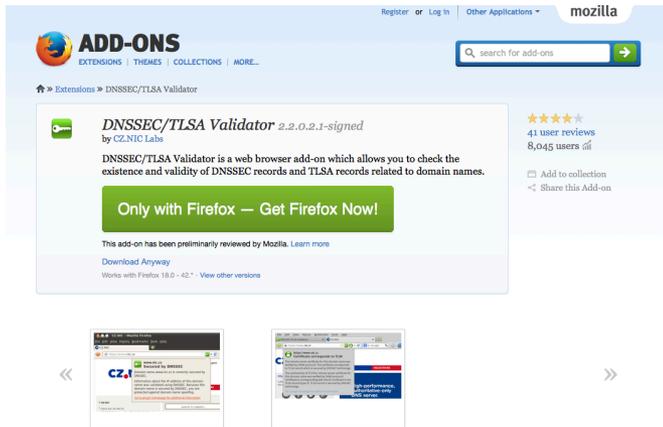
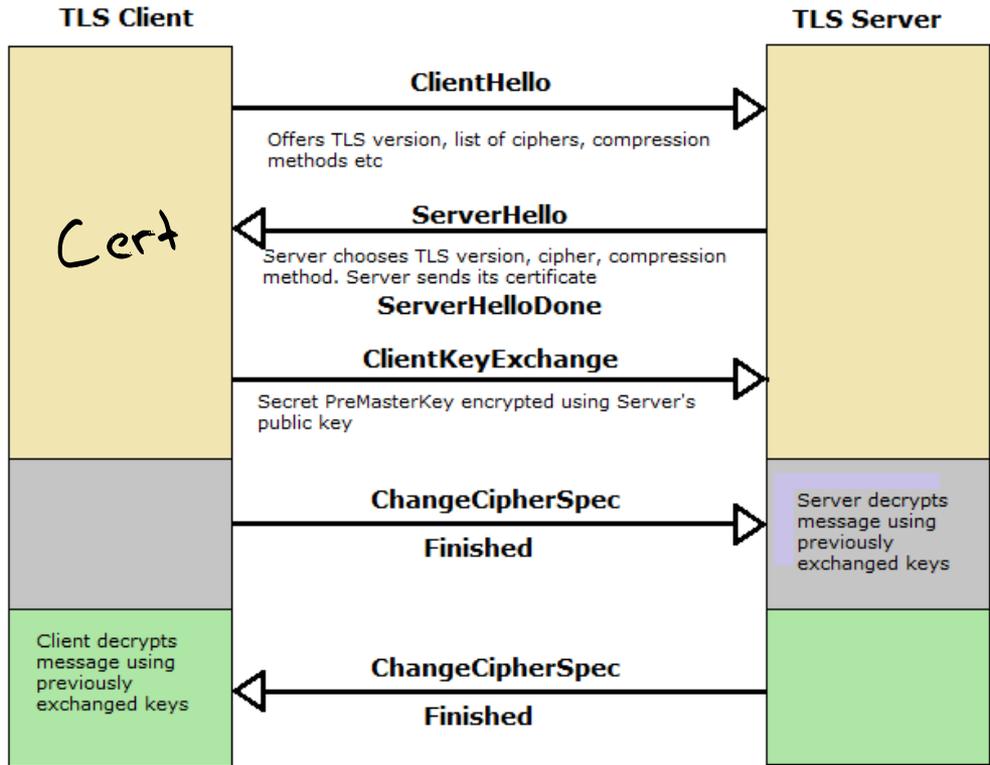
TLS with DANE

- 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

DNS Name

TLSA query



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 displayed 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.

- ★ Add-on home page
- ★ Support site
- ★ Support E-mail

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

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

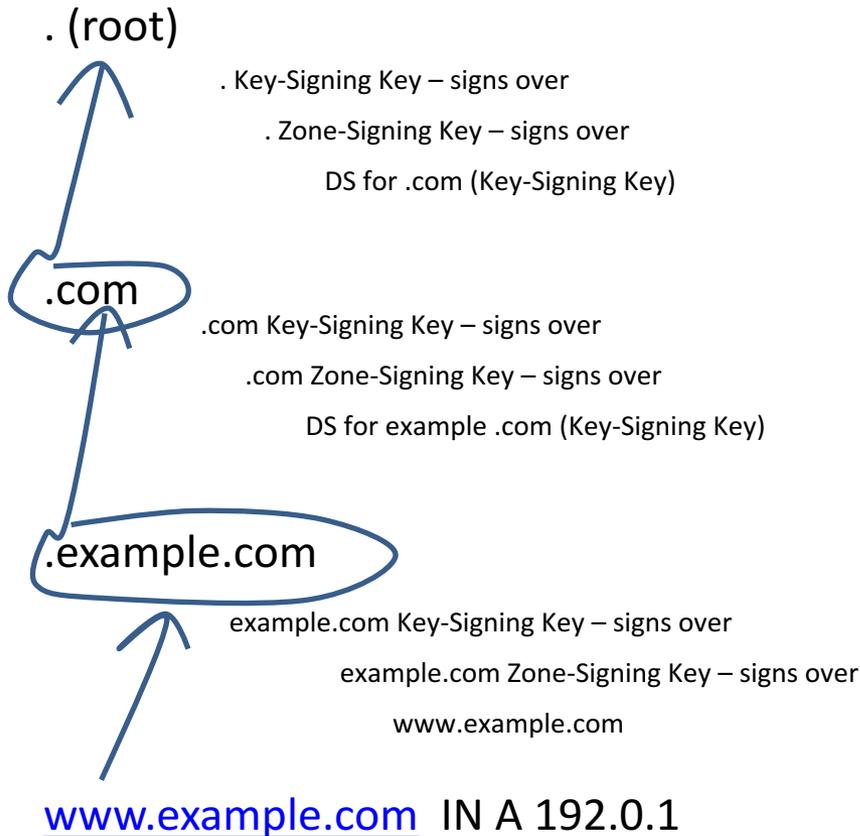
- .com Key-Signing Key – signs over
 - .com Zone-Signing Key – signs over
 - DS for example .com (Key-Signing Key)

.example.com

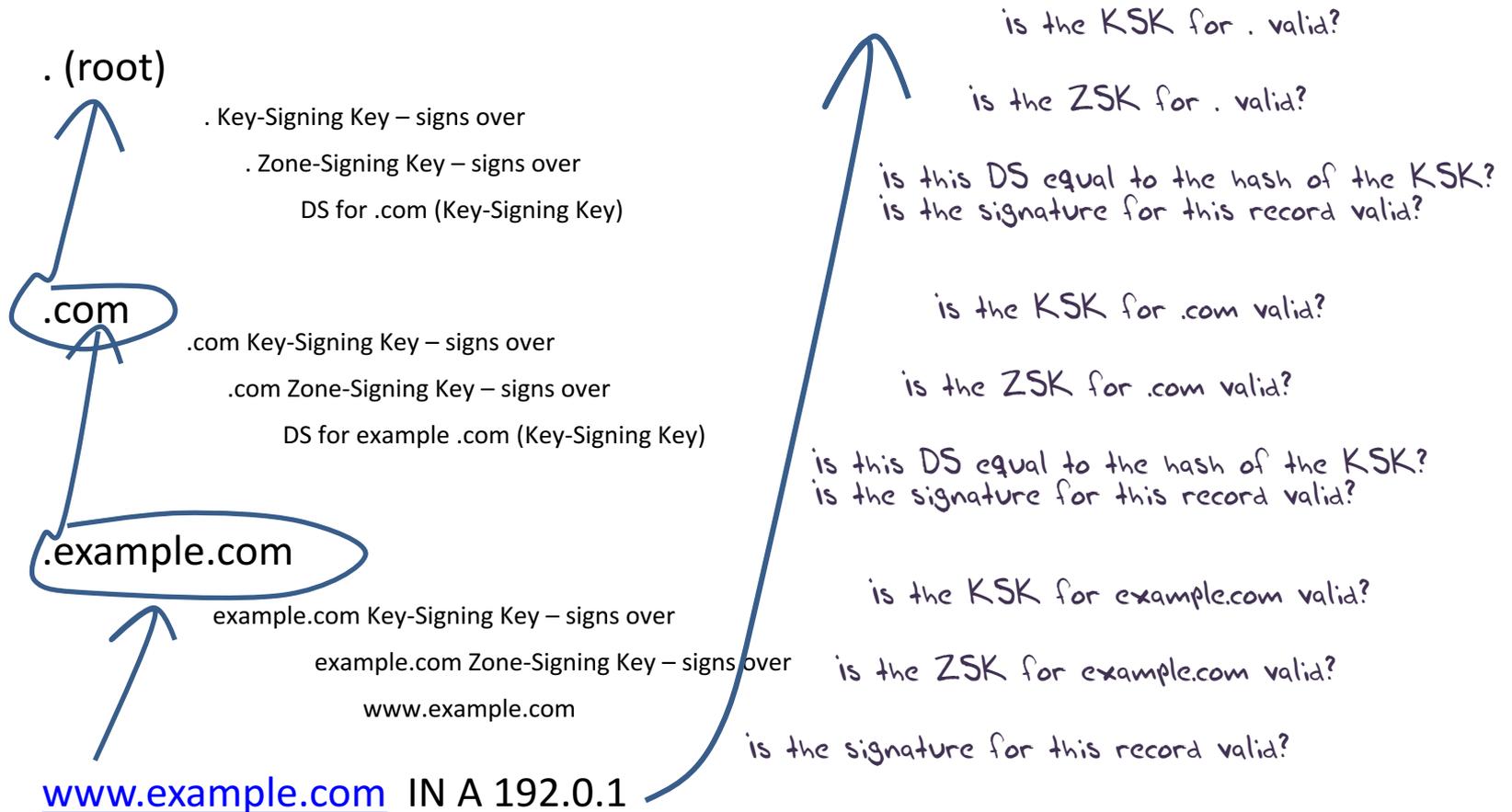
- example.com Key-Signing Key – signs over
 - example.com Zone-Signing Key – signs over
 - www.example.com

www.example.com

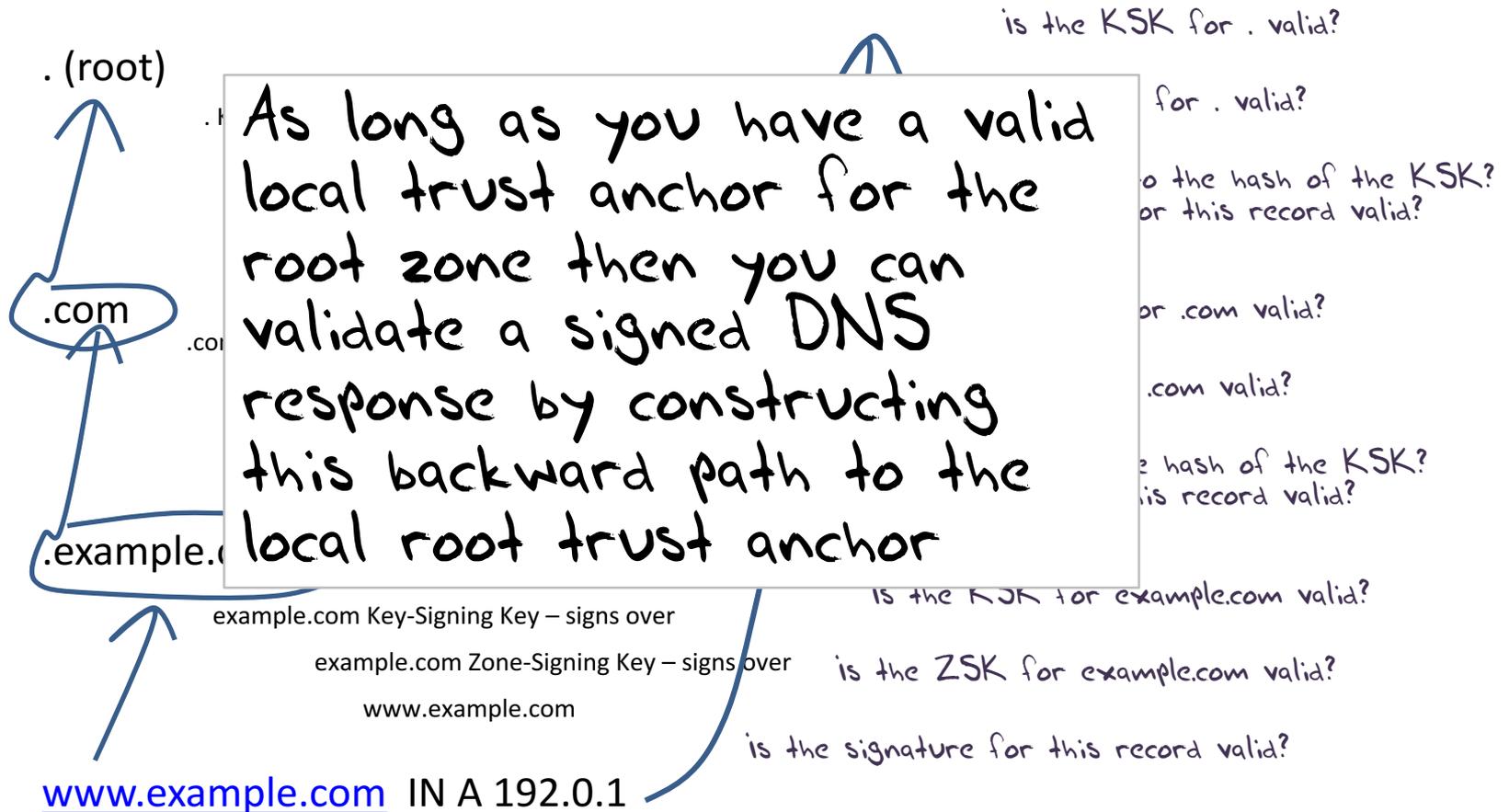
DNSSEC Interlocking Signatures



DNSSEC Interlocking Signatures



DNSSEC Interlocking Signatures



DANE + DNSSEC

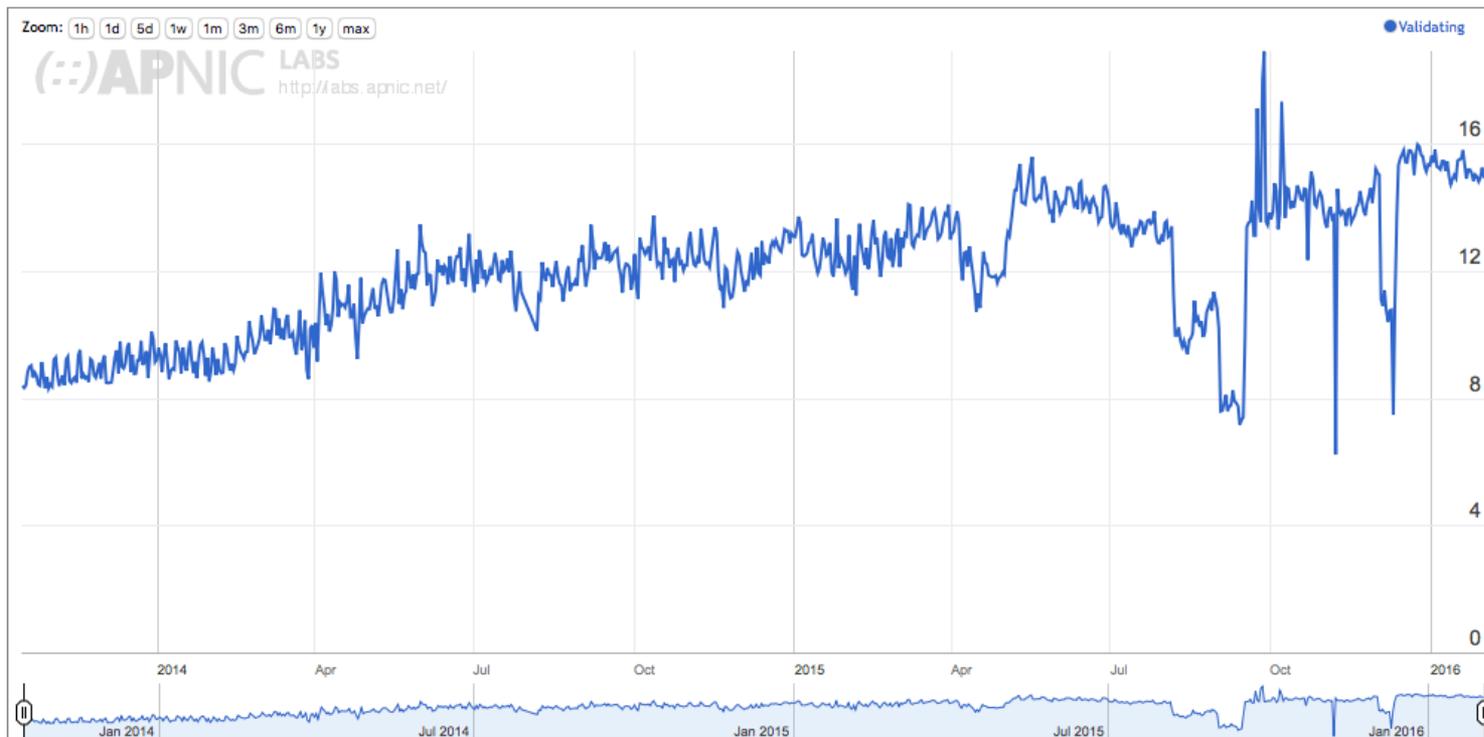
- Query the DNS for the TLSA record of the domain name and ask for the DNSSEC signature to be included in the response
- Validate the signature to ensure that you have an unbroken signature chain to the root trust point
- At this point you can accept the TLSA record as the authentic record, and set up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

Use of DNSSEC Validation for World (XA)



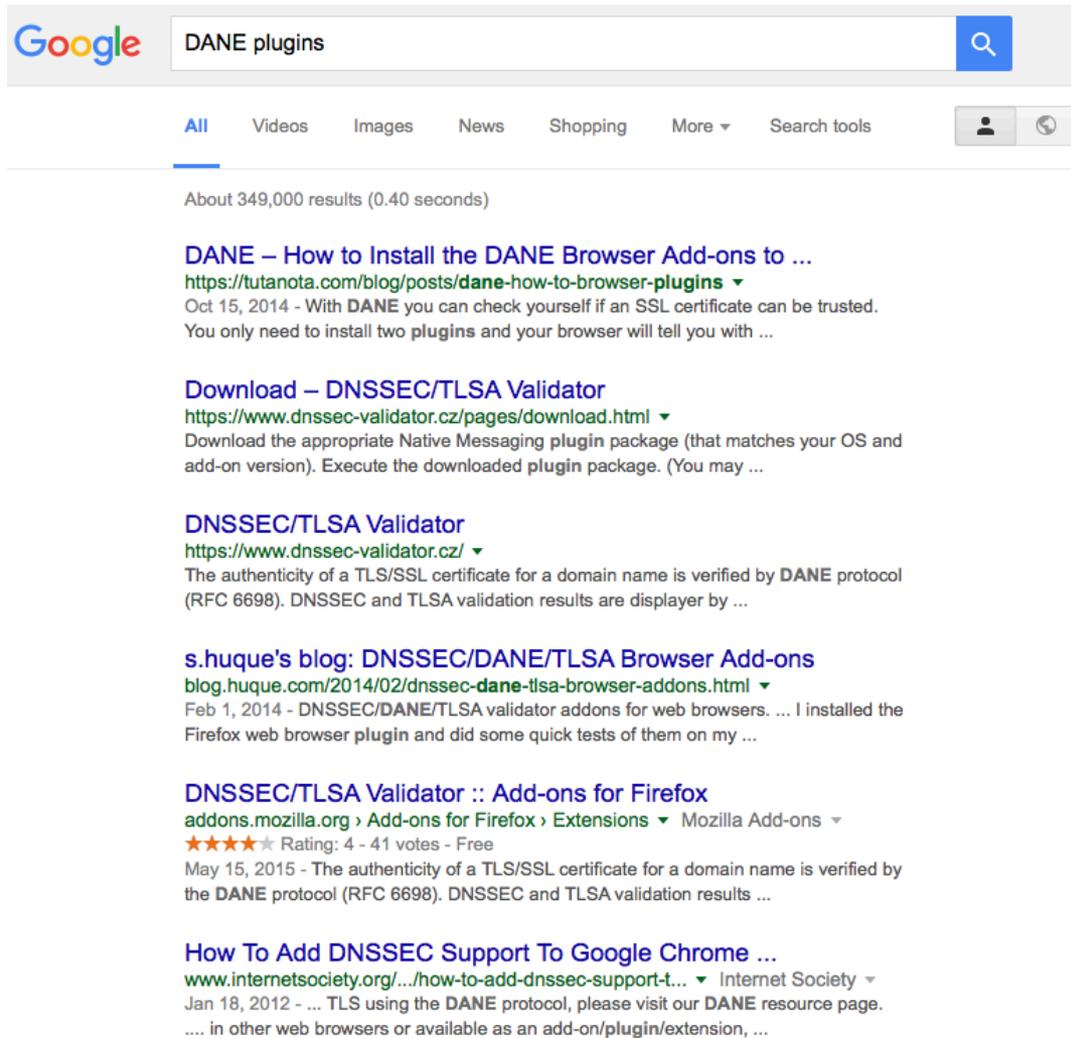
stats.labs.apnic.net/dnssec/XA

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?



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!

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?