It's Time to Fix HTTPS

Yes, really.

Chris Palmer
noncombatant.org

Ideas developed with
Seth Schoen and Peter Eckersley
eff.org

Please note that I do not speak for any of my past, present, or future employers.

Special thanks to

Andy Steingruebl (PayPal)
and
Christopher Soghoian
for valuable discussion

Jesse Burns (iSEC Partners) and Peter
for launching the HTTPS survey

Global PKI,
as currently implemented in browsers,
does not work.

Everyday people do not understand the browser PKI security model.

Nor do developers.

Nor do operations/administrators.

Usability (for all types of users) is the number one security problem on the internet right now.

A key problem is *perverse incentives*. Alice, Bob, and Trent do not share the same goals, means, and limitations.

Perverse Incentives: Certificate Authorities

CAs are incented to sell lots of certs at any price; to stay in the browsers' trust root; to stay in the good graces of law enforcement/government.

The result is a race to the bottom: When you hit $9.99, go back to the top and zoom down the hill again.

("Extended validation" is the same as "1990s validation".)

The result is that meaningless certifications are common.

CAs will sign almost anything (non-FQDNs…),
weak algorithms live too long,
and so on.

"I'll pay you to give someone else a lemon."

Verisign also provides
CALEA compliance services…

Perverse Incentives: Browser Vendors

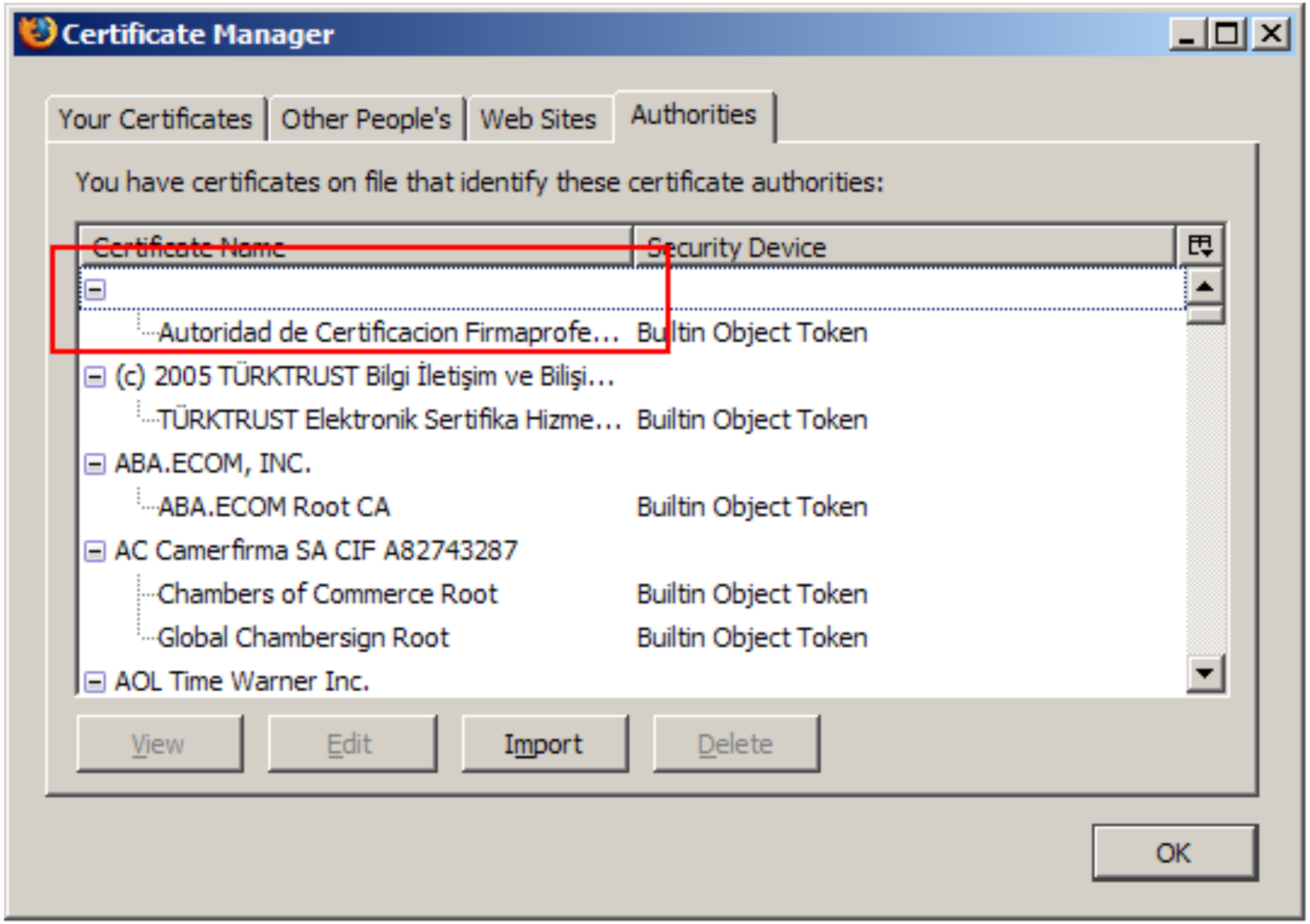
Browser vendors are incented to make sure that scary warnings are not their fault; to be fast, easy to use; to make internet commerce possible, even easy; to ship the spiffy new version before competitor does; to avoid raising millennia-old epistemological and ontological conundra.

As a result, browser vendors accept any CA into the trust root. They avoid raising even true positive warnings (including for, um, HTTP), because some/many might turn out to be false.

(I don't have an explanation for Firefox' jihad against self-signed certificates, however.)

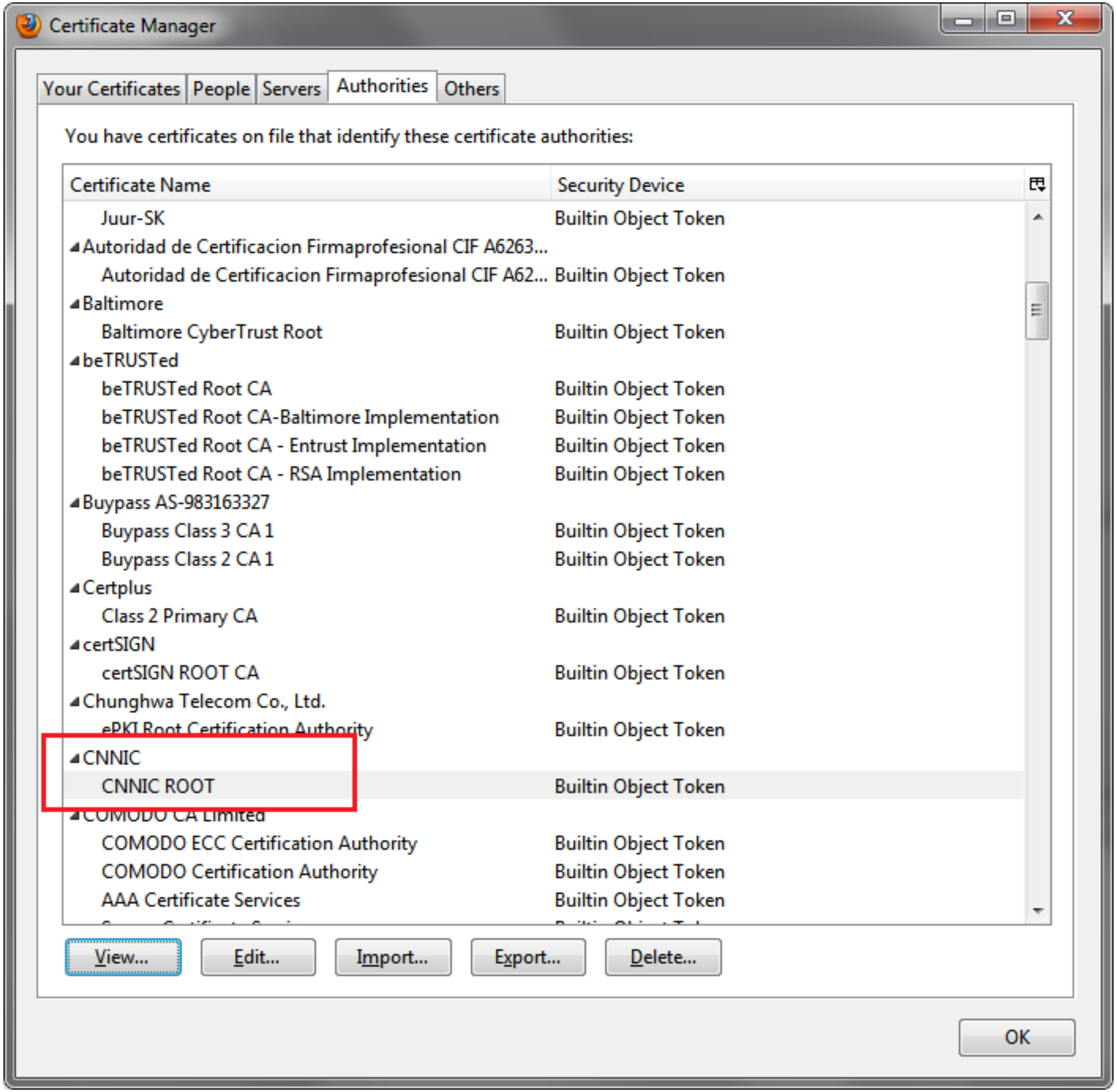
Sidebar:

The browser is the ultimate "CA". It is also the least trustworthy.



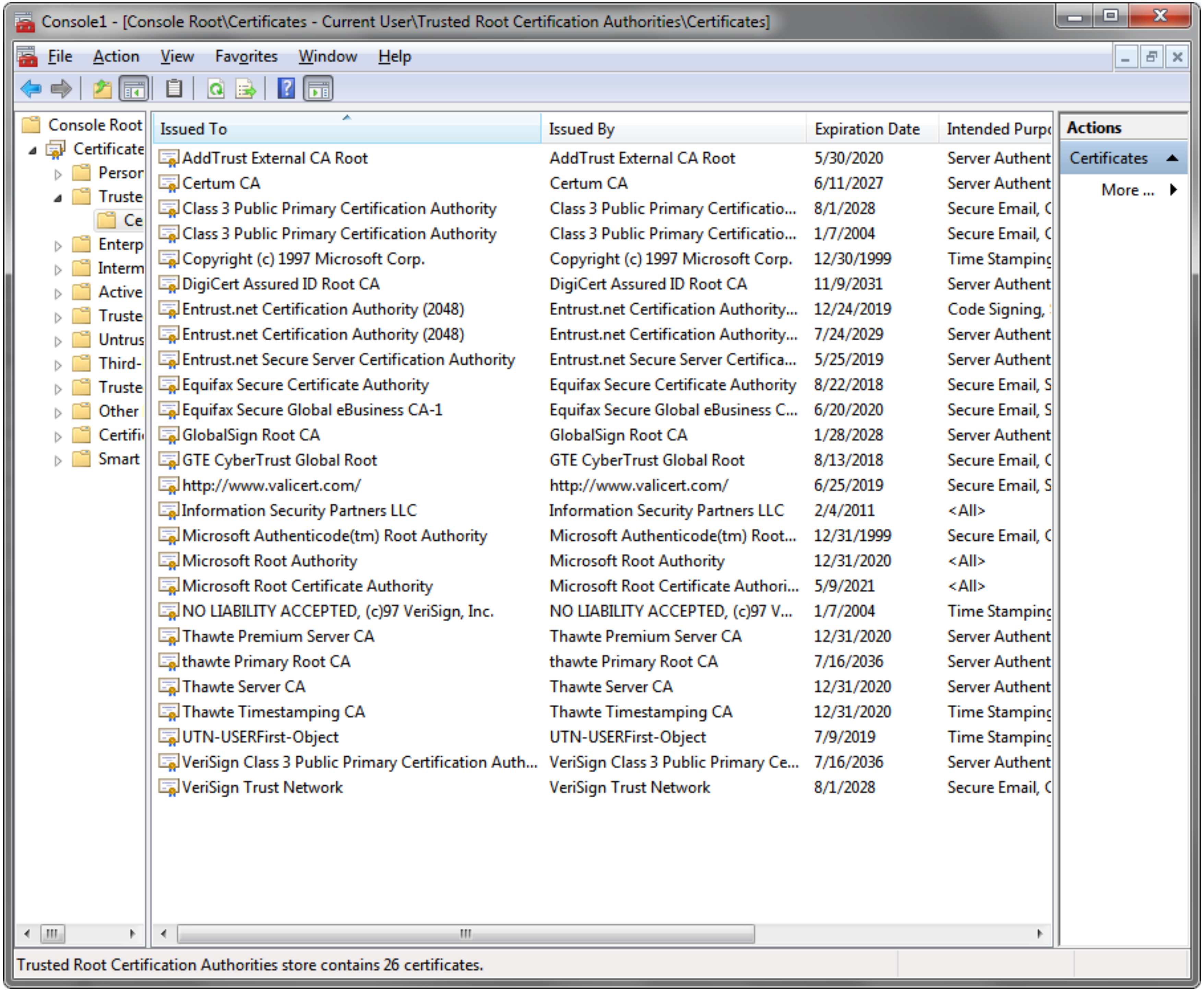
You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
⊟	
Autoridad de Certificacion Firmaprofe...	Builtin Object Token
⊟ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişi...	
TÜRKTRUST Elektronik Sertifika Hizme...	Builtin Object Token
⊟ ABA.ECOM, INC.	
ABA.ECOM Root CA	Builtin Object Token
⊟ AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
⊟ AOL Time Warner Inc.	



You have certificates on file that identify these certificate authorities:

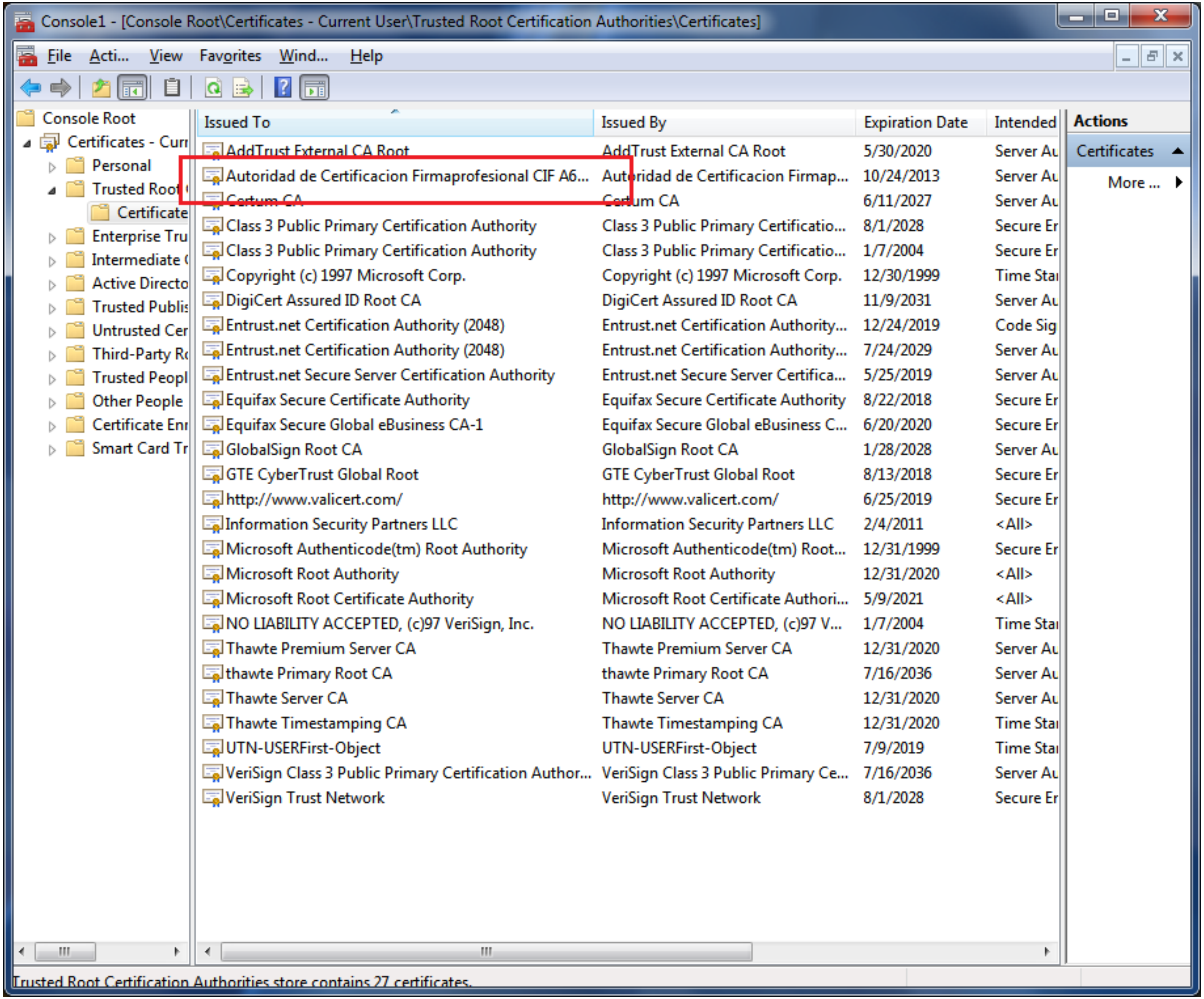
Certificate Name	Security Device
Juur-SK	Builtin Object Token
◢ Autoridad de Certificacion Firmaprofesional CIF A6263...	
Autoridad de Certificacion Firmaprofesional CIF A62...	Builtin Object Token
◢ Baltimore	
Baltimore CyberTrust Root	Builtin Object Token
◢ beTRUSTed	
beTRUSTed Root CA	Builtin Object Token
beTRUSTed Root CA-Baltimore Implementation	Builtin Object Token
beTRUSTed Root CA - Entrust Implementation	Builtin Object Token
beTRUSTed Root CA - RSA Implementation	Builtin Object Token
◢ Buypass AS-983163327	
Buypass Class 3 CA 1	Builtin Object Token
Buypass Class 2 CA 1	Builtin Object Token
◢ Certplus	
Class 2 Primary CA	Builtin Object Token
◢ certSIGN	
certSIGN ROOT CA	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
AAA Certificate Services	Builtin Object Token



Issued To	Issued By	Expiration Date	Intended Purp
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authent
Certum CA	Certum CA	6/11/2027	Server Authent
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, C
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, C
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authent
Entrust.net Certification Authority (2048)	Entrust.net Certification Authority...	12/24/2019	Code Signing,
Entrust.net Certification Authority (2048)	Entrust.net Certification Authority...	7/24/2029	Server Authent
Entrust.net Secure Server Certification Authority	Entrust.net Secure Server Certifica...	5/25/2019	Server Authent
Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	8/22/2018	Secure Email, S
Equifax Secure Global eBusiness CA-1	Equifax Secure Global eBusiness C...	6/20/2020	Secure Email, S
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authent
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, C
http://www.valicert.com/	http://www.valicert.com/	6/25/2019	Secure Email, S
Information Security Partners LLC	Information Security Partners LLC	2/4/2011	<All>
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, C
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>
Microsoft Root Certificate Authority	Microsoft Root Certificate Authori...	5/9/2021	<All>
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authent
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Authent
Thawte Server CA	Thawte Server CA	12/31/2020	Server Authent
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Time Stamping
VeriSign Class 3 Public Primary Certification Auth...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Authent
VeriSign Trust Network	VeriSign Trust Network	8/1/2028	Secure Email, C

Trusted Root Certification Authorities store contains 26 certificates.

Just get CSRF'd into visiting https://www.firmaprofesional.com/ and...



Issued To	Issued By	Expiration Date	Intended
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Au
Autoridad de Certificacion Firmaprofesional CIF A6...	Autoridad de Certificacion Firmap...	10/24/2013	Server Au
Certum CA	Certum CA	6/11/2027	Server Au
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certificatio...	8/1/2028	Secure Er
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certificatio...	1/7/2004	Secure Er
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stai
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Au
Entrust.net Certification Authority (2048)	Entrust.net Certification Authority...	12/24/2019	Code Sig
Entrust.net Certification Authority (2048)	Entrust.net Certification Authority...	7/24/2029	Server Au
Entrust.net Secure Server Certification Authority	Entrust.net Secure Server Certifica...	5/25/2019	Server Au
Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	8/22/2018	Secure Er
Equifax Secure Global eBusiness CA-1	Equifax Secure Global eBusiness C...	6/20/2020	Secure Er
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Au
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Er
http://www.valicert.com/	http://www.valicert.com/	6/25/2019	Secure Er
Information Security Partners LLC	Information Security Partners LLC	2/4/2011	<All>
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Er
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>
Microsoft Root Certificate Authority	Microsoft Root Certificate Authori...	5/9/2021	<All>
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stai
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Au
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Au
Thawte Server CA	Thawte Server CA	12/31/2020	Server Au
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stai
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Time Stai
VeriSign Class 3 Public Primary Certification Author...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Au
VeriSign Trust Network	VeriSign Trust Network	8/1/2028	Secure Er

Trusted Root Certification Authorities store contains 27 certificates.

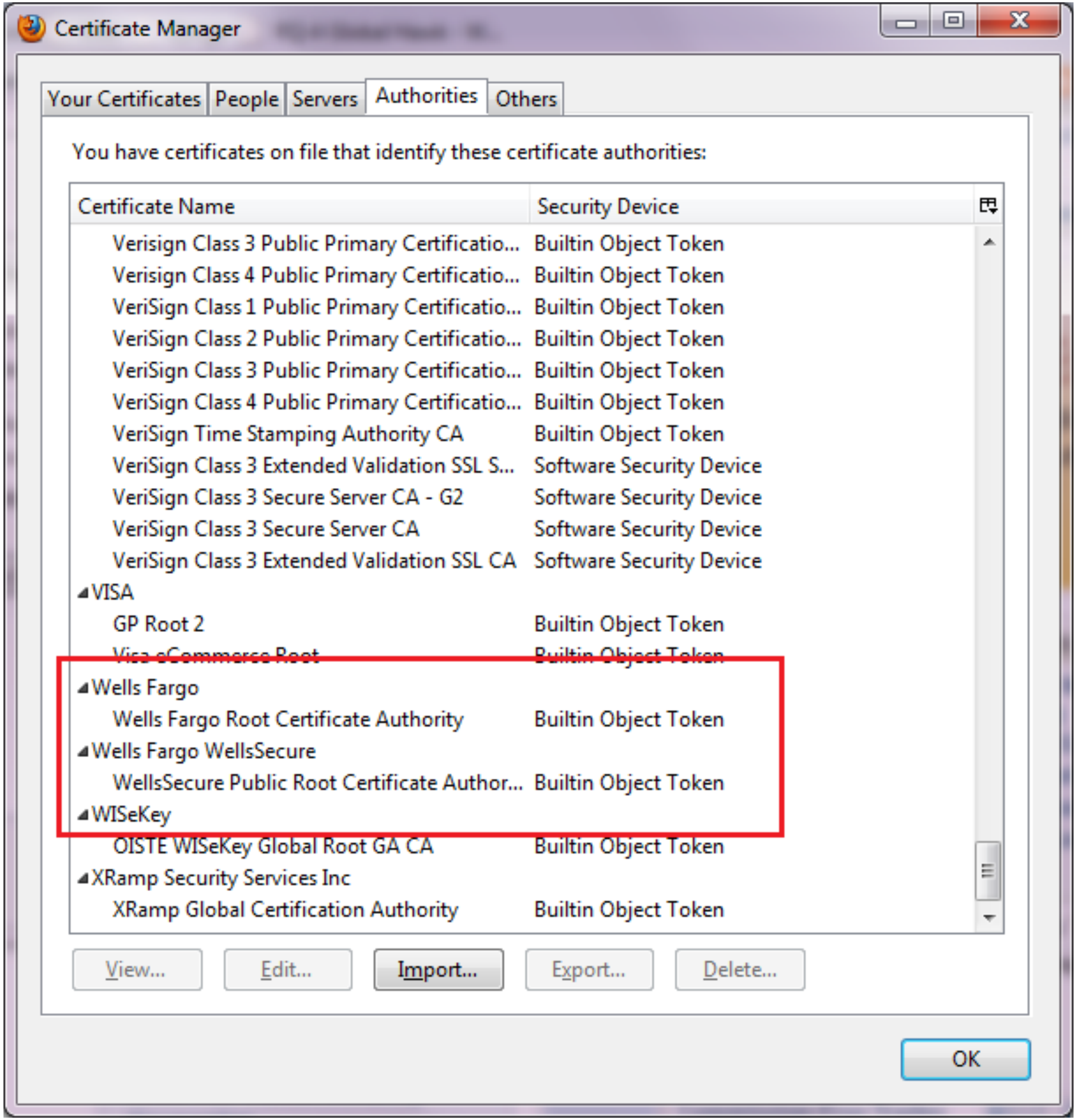
Quiz Time!

If IE runs as Low IL and is UAC virtualized, how can it silently update the cert store?

A Medium-IL broker process does the work of updating the user's (not the machine's) CA trust store.

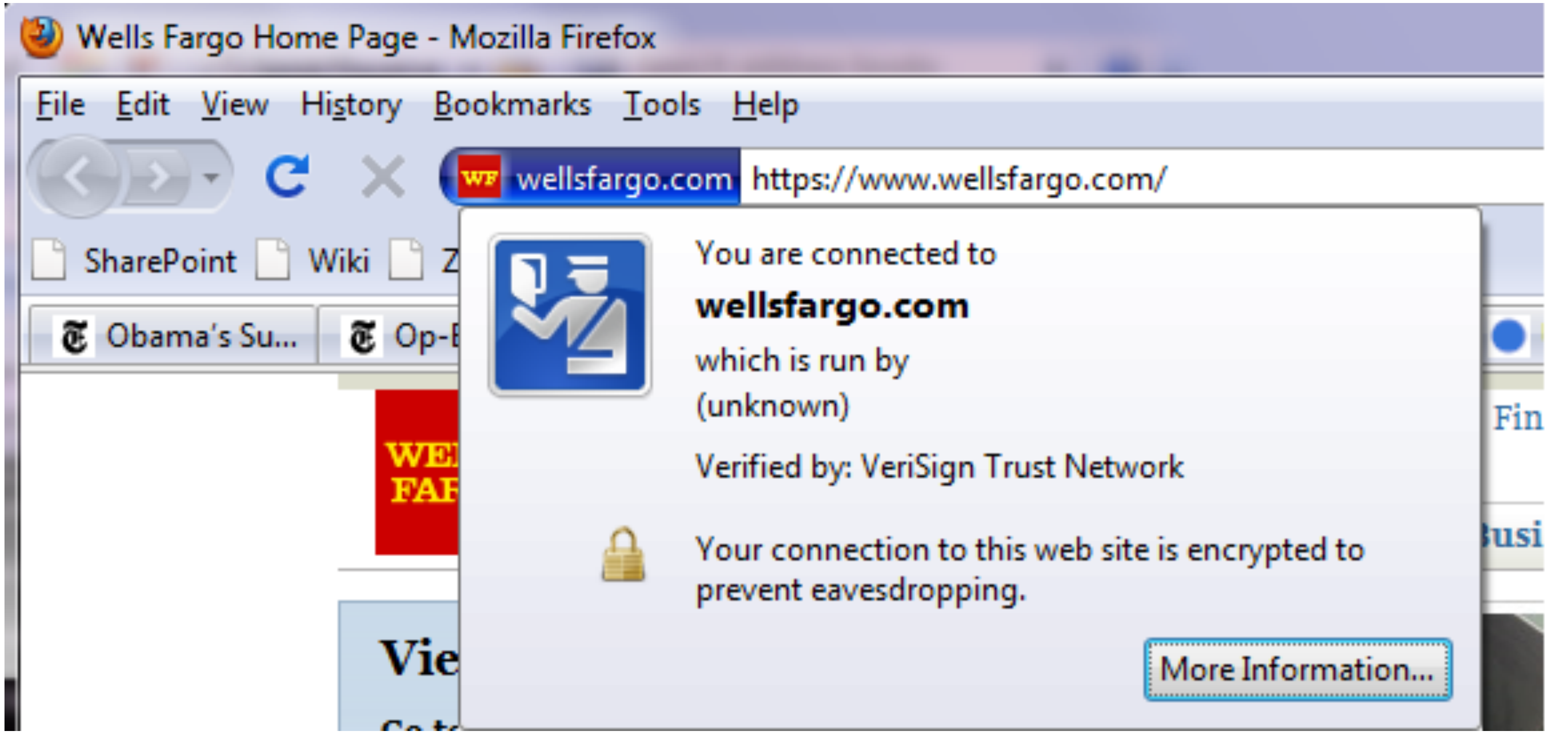
Sounds like a High-IL thing to do, if you ask me.

Especially with no user notification or interaction!



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
Verisign Class 3 Public Primary Certificatio...	Builtin Object Token
Verisign Class 4 Public Primary Certificatio...	Builtin Object Token
VeriSign Class 1 Public Primary Certificatio...	Builtin Object Token
VeriSign Class 2 Public Primary Certificatio...	Builtin Object Token
VeriSign Class 3 Public Primary Certificatio...	Builtin Object Token
VeriSign Class 4 Public Primary Certificatio...	Builtin Object Token
VeriSign Time Stamping Authority CA	Builtin Object Token
VeriSign Class 3 Extended Validation SSL S...	Software Security Device
VeriSign Class 3 Secure Server CA - G2	Software Security Device
VeriSign Class 3 Secure Server CA	Software Security Device
VeriSign Class 3 Extended Validation SSL CA	Software Security Device
◢VISA	
GP Root 2	Builtin Object Token
Visa eCommerce Root	Builtin Object Token
◢Wells Fargo	
Wells Fargo Root Certificate Authority	Builtin Object Token
◢Wells Fargo WellsSecure	
WellsSecure Public Root Certificate Author...	Builtin Object Token
◢WISeKey	
OISTE WISeKey Global Root GA CA	Builtin Object Token
◢XRamp Security Services Inc	
XRamp Global Certification Authority	Builtin Object Token



Wells Fargo Home Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
wellsfargo.com
https://www.wellsfargo.com/
SharePoint
Wiki
Obama's Su...
Op-
More Information...

You are connected to

wellsfargo.com

which is run by

(unknown)

Verified by: VeriSign Trust Network

Your connection to this web site is encrypted to prevent eavesdropping.

Perverse Incentives: Site Operators

Site operators are incented to pay the lowest possible cost for a lemon; to shift blame and liability to anyone else: CA, user, whoever; to never be unavailable.

As a result, they get a perfectly good lemon for a very fair price. Users have no idea if they are talking to the real site. The costs of fraud, phishing, MITM rise. Operators may punt those back to the user.

Perverse Incentives: People

People are incented to use the internet at reasonable cost, without having to understand things not even security experts understand; to not pay the costs of fraud that is not their fault; to talk to the true site; to have confidentiality and integrity.

The result?

If you're not a wolf, you're a lamb.

The Basiji, the Great Firewall operators, the NSA, spammers, phishers, dreadlocked sea captains, and script kiddies can too-easily MITM people.

Banks may pass the costs back down to people --- that "maximum $50 liability" means the liability is just hidden.

Solution(s)

Prime Directive: Usability

Usability requires empathy.

Change the security model to be one that people can understand.

If people don't understand it,
we engineered it wrong.

Secure usability requires
security assertions that:

- Can be stated in one sentence of colloquial English.
- Could possibly be true.
- Could possibly be computed.

Let's start more modestly:

A security model that requires
only one advanced degree to understand.

More-Usable Security Assertions

"This is almost certainly the same server you connected with yesterday."

"You've been connecting to almost certainly the same server all month."

"This is probably the same server you connected with yesterday."

"Something seems fishy; this is probably not the same server you connected with yesterday. You should call or visit your bank/whatever to be sure nothing bad has happened."

You guessed it: I prefer TOFU/POP.

(Trust On First Use;
Persistence of Pseudonym)

The server's cryptographic identifier (its certificate and the certificate's signatures) is its pseudonym.

There are some objections to the TOFU/POP approach, however.

I'll consider three famous objections now.

"But TOFU/POP Doesn't Scale"

Global PKI only "scales" if by "scale" you mean "scales unsafely and unusably".

TOFU/POP does better than that.

More importantly, TOFU/POP works
--- unlike global PKI.

After all, you (developer, admin) have been using TOFU/POP to log into the server as root. Maybe, just maybe, it's also good enough for non-root people too?

A key part of the "doesn't scale" argument is the *secure introduction* problem. And it's true that TOFU/POP suffers from the problem.

But PKI also suffers from the problem (HTTP by default, without STS).

It's a considerably less-bad problem than the status quo: a false sense of security for PKI users.

"But TOFU/POP Doesn't Adapt"

Another criticism of TOFU/POP is that it does not adapt to legitimate changes in the server's pseudonym.

(Actually, much of the "need" to change is due to CA problems. Oh, and actual hacks. It's hard for a user to tell the difference between legitimate certificate change and hacks.)

We therefore propose a new heuristic: "trustiness".

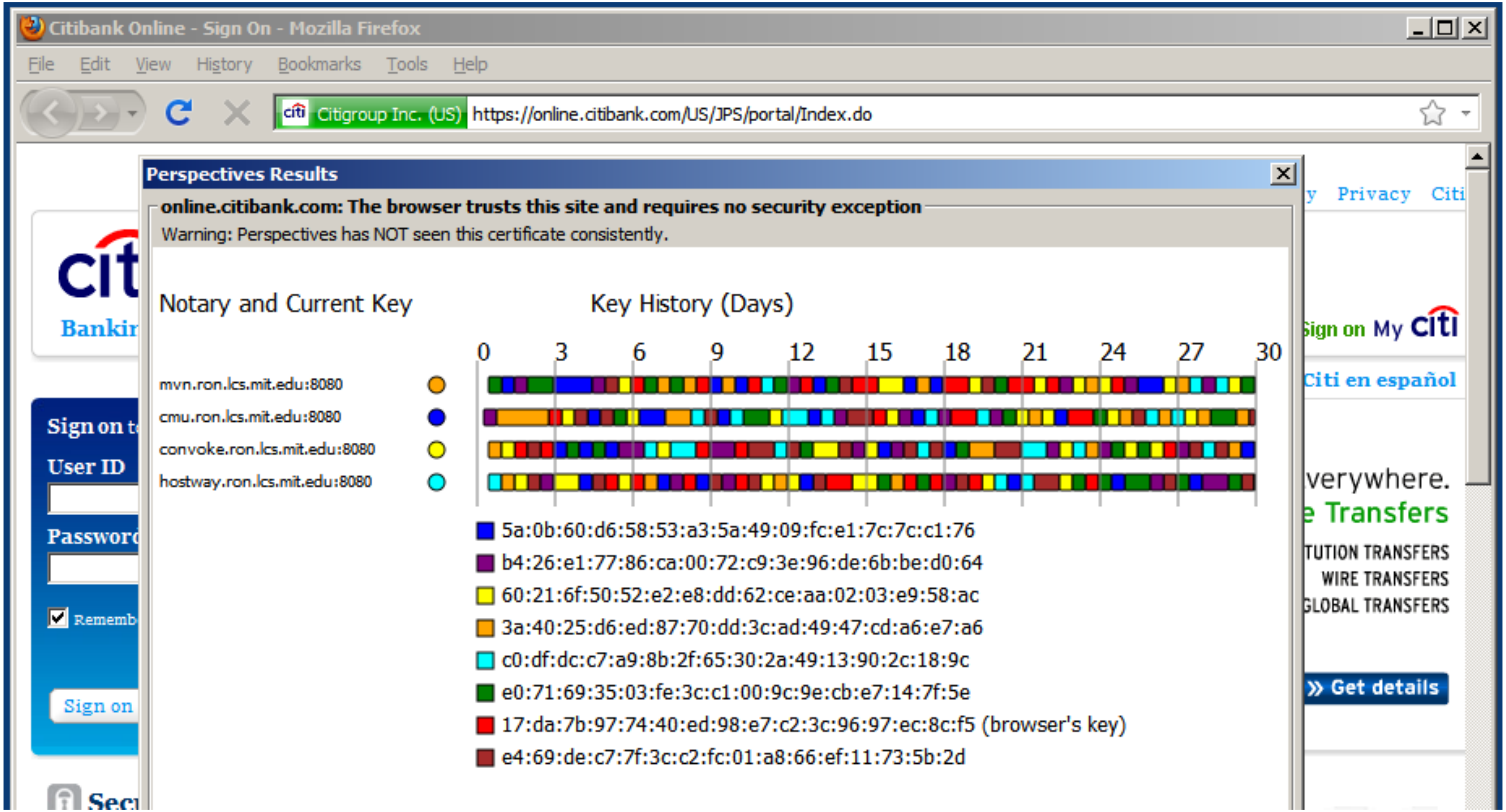
We try to paper over the adaptation problem by gathering information from many sources. Judge the likelihood that the change is OK.

"But I don't have a 1:1 mapping hostname:certificate"

We call this The Citibank Problem: every server in the cluster has a different certificate.

(Why are they paying for that?
Some people have a rule to "never move/copy a private key", so each server/load balancer gets its own cert.)

The downside of this is that,
combined with the
untrsutworthiness of CAs,
it is very hard to know who we
are talking to.



Perspectives Results

online.citibank.com: The browser trusts this site and requires no security exception

Warning: Perspectives has NOT seen this certificate consistently.

Notary and Current Key

Key History (Days)

mvn.ron.lcs.mit.edu:8080	🟠
cmu.ron.lcs.mit.edu:8080	🔵
convoke.ron.lcs.mit.edu:8080	🟡
hostway.ron.lcs.mit.edu:8080	●

🟦 5a:0b:60:d6:58:53:a3:5a:49:09:fc:e1:7c:7c:c1:76

🟪 b4:26:e1:77:86:ca:00:72:c9:3e:96:de:6b:be:d0:64

🟨 60:21:6f:50:52:e2:e8:dd:62:ce:aa:02:03:e9:58:ac

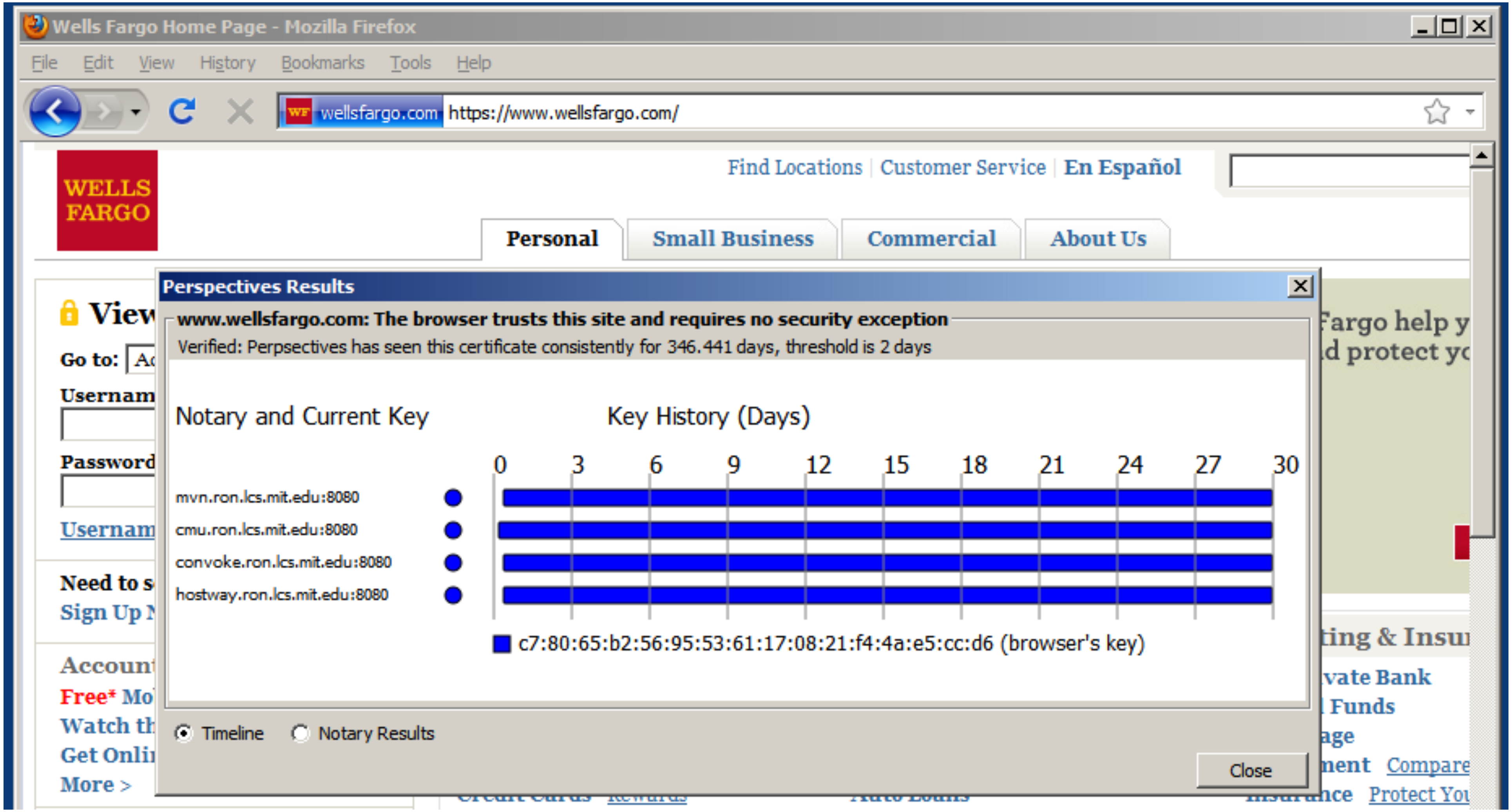
🟧 3a:40:25:d6:ed:87:70:dd:3c:ad:49:47:cd:a6:e7:a6

■ c0:df:dc:c7:a9:8b:2f:65:30:2a:49:13:90:2c:18:9c

🟩 e0:71:69:35:03:fe:3c:c1:00:9c:9e:cb:e7:14:7f:5e

🟥 17:da:7b:97:74:40:ed:98:e7:c2:3c:96:97:ec:8c:f5 (browser's key)

🟫 e4:69:de:c7:7f:3c:c2:fc:01:a8:66:ef:11:73:5b:2d


Wells Fargo Home Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
wellsfargo.com
https://www.wellsfargo.com/
WELLS FARGO
Find Locations | Customer Service | En Español
Personal
Small Business
Commercial
About Us
Perspectives Results
Timeline
Notary Results
Close

www.wellsfargo.com: The browser trusts this site and requires no security exception

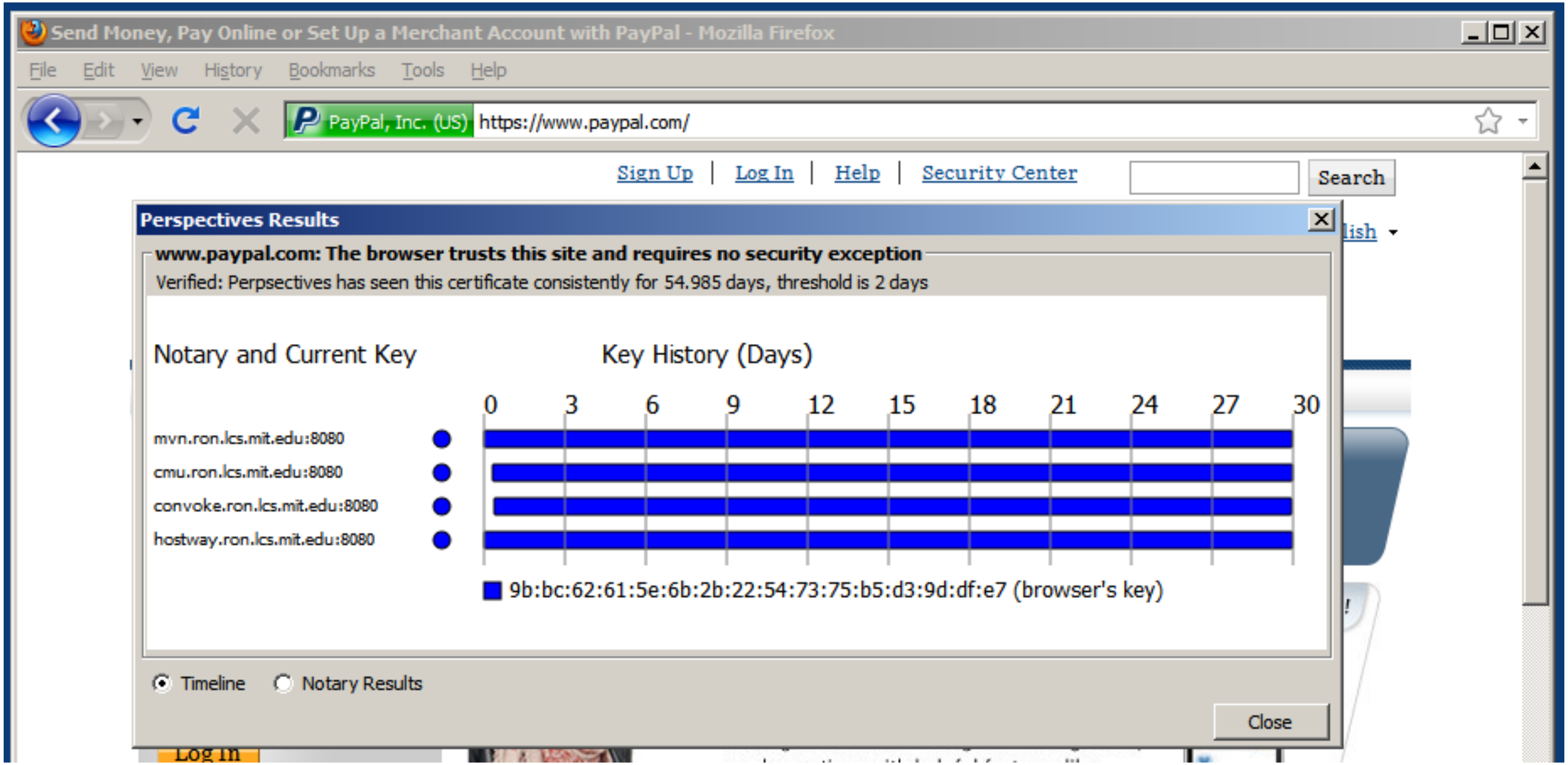
Verified: Perpsectives has seen this certificate consistently for 346.441 days, threshold is 2 days

Notary and Current Key

Key History (Days)

0
3
6
9
12
15
18
21
24
27
30
mvn.ron.lcs.mit.edu:8080 ●
cmu.ron.lcs.mit.edu:8080 ●
convoke.ron.lcs.mit.edu:8080 ●
hostway.ron.lcs.mit.edu:8080 ●
■ c7:80:65:b2:56:95:53:61:17:08:21:f4:4a:e5:cc:d6 (browser's key)

● Timeline ○ Notary Results

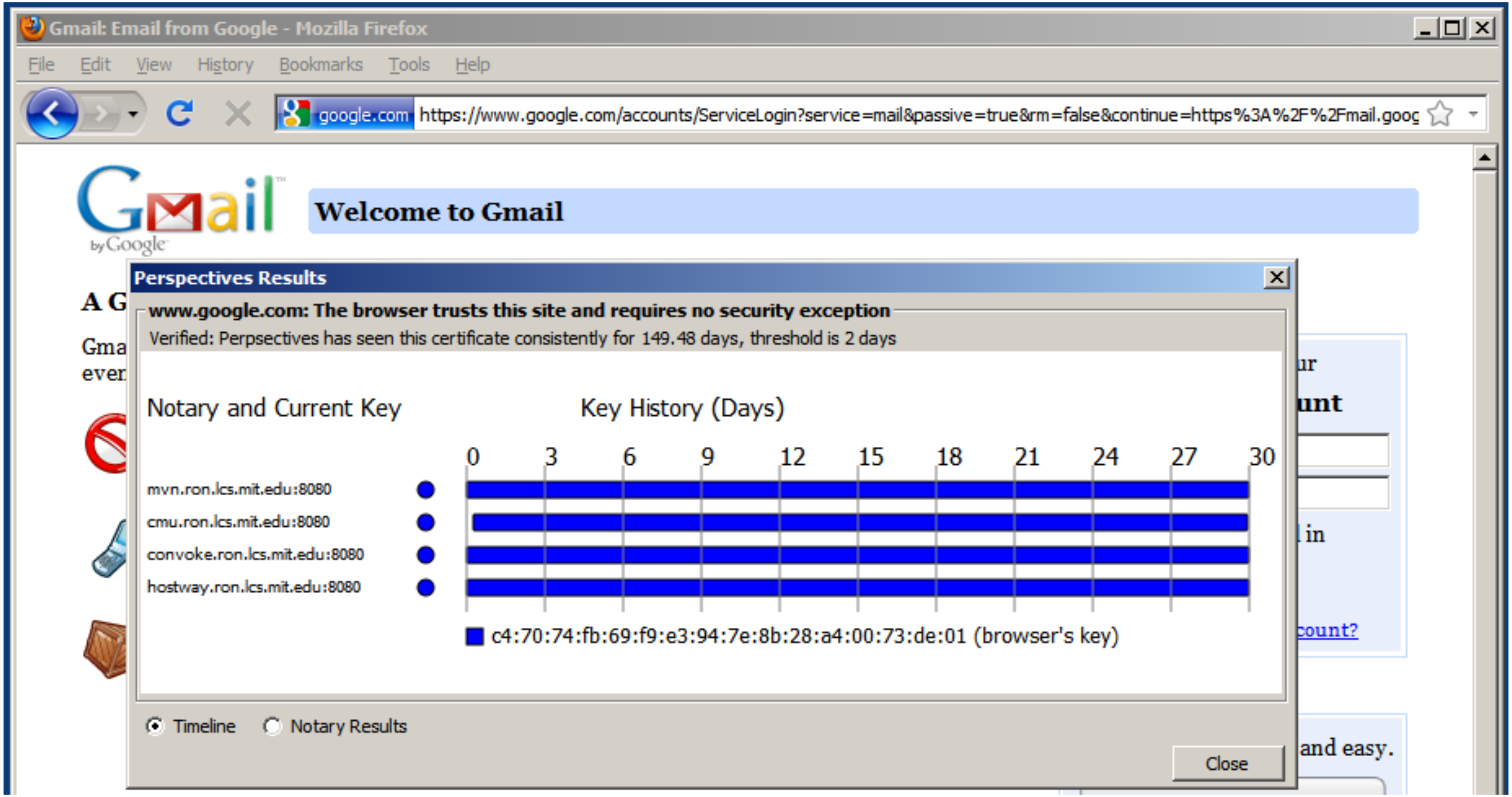


www.paypal.com: The browser trusts this site and requires no security exception

Verified: Perspectives has seen this certificate consistently for 54.985 days, threshold is 2 days

🟦 9b:bc:62:61:5e:6b:2b:22:54:73:75:b5:d3:9d:df:e7 (browser's key)

● Timeline ○ Notary Results



https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=https%3A%2F%2Fmail.goog

Welcome to Gmail

Perspectives Results

www.google.com: The browser trusts this site and requires no security exception

Verified: Perpsectives has seen this certificate consistently for 149.48 days, threshold is 2 days

mvn.ron.lcs.mit.edu:8080 ●

cmu.ron.lcs.mit.edu:8080 ●

convoke.ron.lcs.mit.edu:8080 ●

hostway.ron.lcs.mit.edu:8080 ●

■ c4:70:74:fb:69:f9:e3:94:7e:8b:28:a4:00:73:de:01 (browser's key)

◉ Timeline ○ Notary Results

Sources of Trustiness

- Infotainment in the X.509 blob
  - Expiry
  - CN == CNAME
  - Identity of signers in chain
  - Quality of signing algorithm
  - Size of public key
  - Duration of validity period
    - Lately I've seen certs that last until 2038.
- Revocation (CRL, OCSP, other?) clues
- Perspectives
  - "You can't fool all the people all the time"

Potential Sources of Trustiness

- DNSSEC
- Monkeysphere, Web of Trust
    - Orderly key transitions
    - Old key (co-)signs new one
- Has the certificate's signer changed?
- Future STS-like mechanisms
    - Statements that the site makes about what clients should expect/expect in the future

Just a Simple Matter of Pseudocode…

```
def trust_cert(cert, origin):
    if (cert trusted for this origin previously):
        if (cert not revoked and cert not expired):
            return Trust
        else:
            return trust_expired_or_revoked(cert, origin)
    elif (new origin)
         return trust_fresh_origin(cert, origin)
    else:
         # new cert for old origin
         return trust_changed_cert(cert, origin)
```

```
def trust_expired_or_revoked_cert(cert, origin)
    if (revoked)
        if (perspectives consensus):
            return Maybe_trust
        else:
            return Probably_MITM
    # expired
    if (no valid cert since expiration):
        # This is probably just a failure to replace
        # an expiring cert
        return Probably_trust
    else:
        return Maybe_trust
```

```
def trust_fresh_origin(cert, origin):
    if (cert not for this origin):
        if (perspectives consensus):
            return Maybe_trust
        else:
            return Probably_MITM
    elif (trusted signer) and (consensus):
        return Trust
    elif (trusted EV signer):
        return Trust
    elif (trusted signer) or (consensus):
       return Probably_trust
```

```
def trust_changed_cert(cert, origin):
    # This is really the hardest case
    if (old cert revoked) or (old cert expiring):
        return trust_fresh_origin(cert, origin)
    elif (perspectives consensus)
        if (trusted signer):
            return Trust
        else:
            return Maybe_trust
    else:    # no consensus
        if (trusted signer)
            if user_opted_for_whitelist and (origin in whitelist):
                return Probably_trust
            else:
                return Maybe_trust
        else:
            return Probably_MITM
```

Obstacles to Improvement

Browser vendors:
"I'm not going to stick
MY neck out!"

Site operators:
"So it's been broken all along,
and we are still in business.
Why change?"

CAs:
"But we love CAs!"

Percival:
"Evite is down."

Muffy:
"What? WHAT?! Omigod, omigod ---" *hyperventilates*

(MC Frontalot's new CD is great)

Signs of Progress

STS

(first step toward HTTPS/SPDY-only!)

Perspectives

Certificate Patrol

Certlock

Google now supports HTTPS for search (https://www.google.com/support/websearch/bin/answer.py?answer=173733&hl=en)

Phrases to Google For

("Web 2.0 Works Cited")

:)

Peter Gutmann's book DRAFT: http://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf

MD5 Considered Harmful Today

Soghoian and Stamm Certified Lies

Firefox Bugzilla CNNIC

Sotirov and Zusman EV Black Hat

Kurt Seifried Breach of Trust

Moxie Marlinspike SSLStrip

Zooko's Triangle

Abandoned root certificate found in Firefox

Nasko Oskov netsekure.org

Thanks for listening!

Questions?