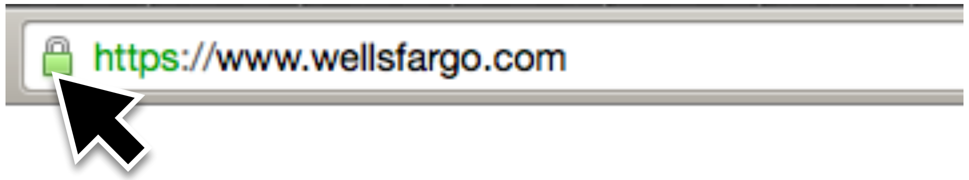
Certificates in the wild

Slides from

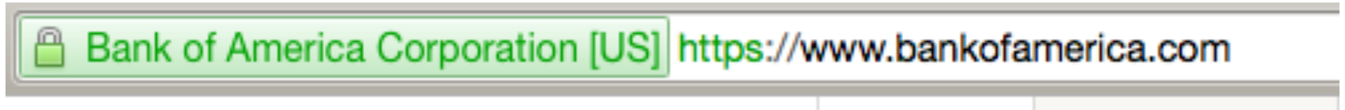
- Dave Levin 414-spring2016
- Michelle Mazurek 414-fall2016

Certificates in the wild

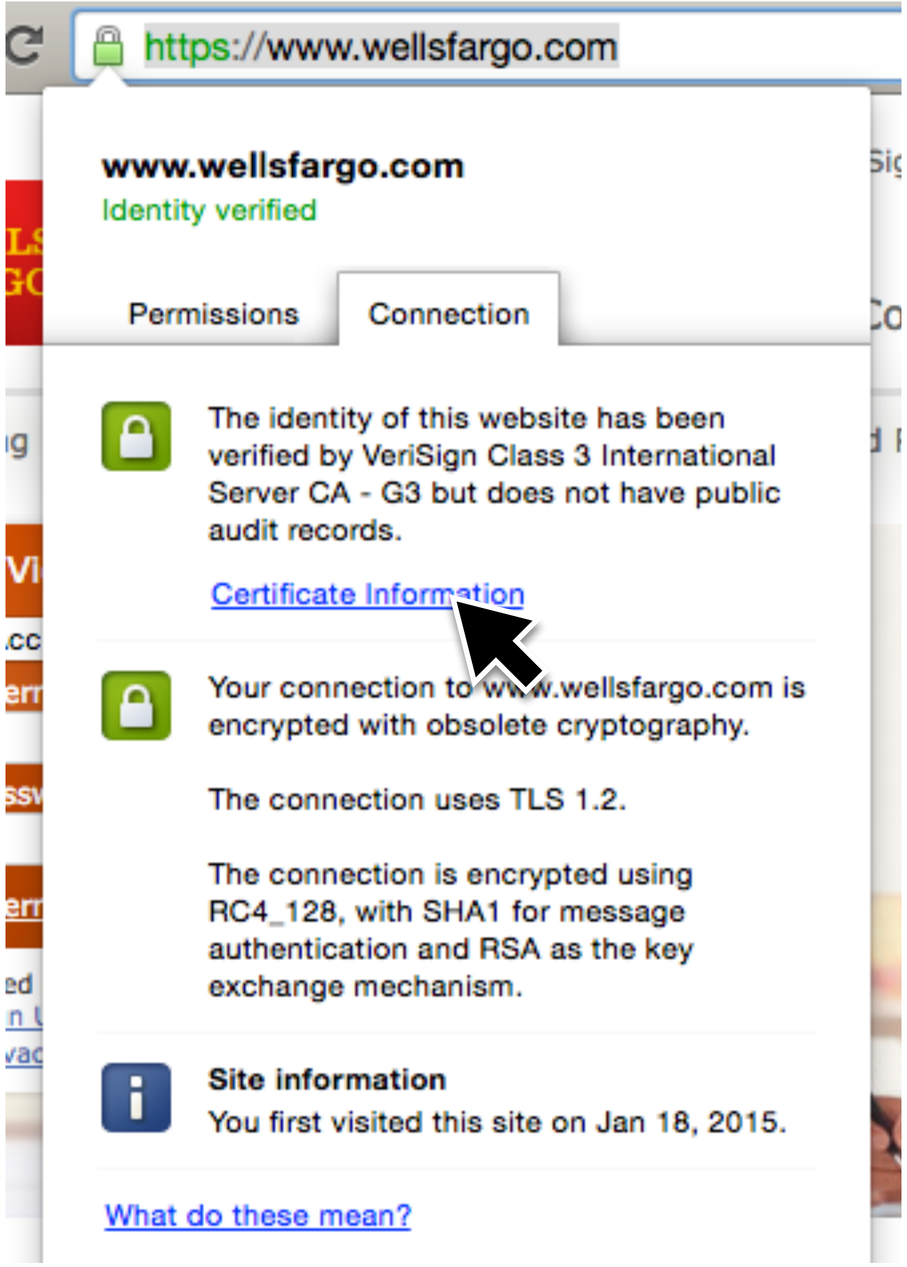
The lock icon indicates that the browser was able to authenticate the other end, i.e., validate its certificate



https://www.wellsfargo.com



Bank of America Corporation [US] https://www.bankofamerica.com



https://www.wellsfargo.com

www.wellsfargo.com

Identity verified

The identity of this website has been verified by VeriSign Class 3 International Server CA - G3 but does not have public audit records.

Certificate Information

Your connection to www.wellsfargo.com is encrypted with obsolete cryptography.

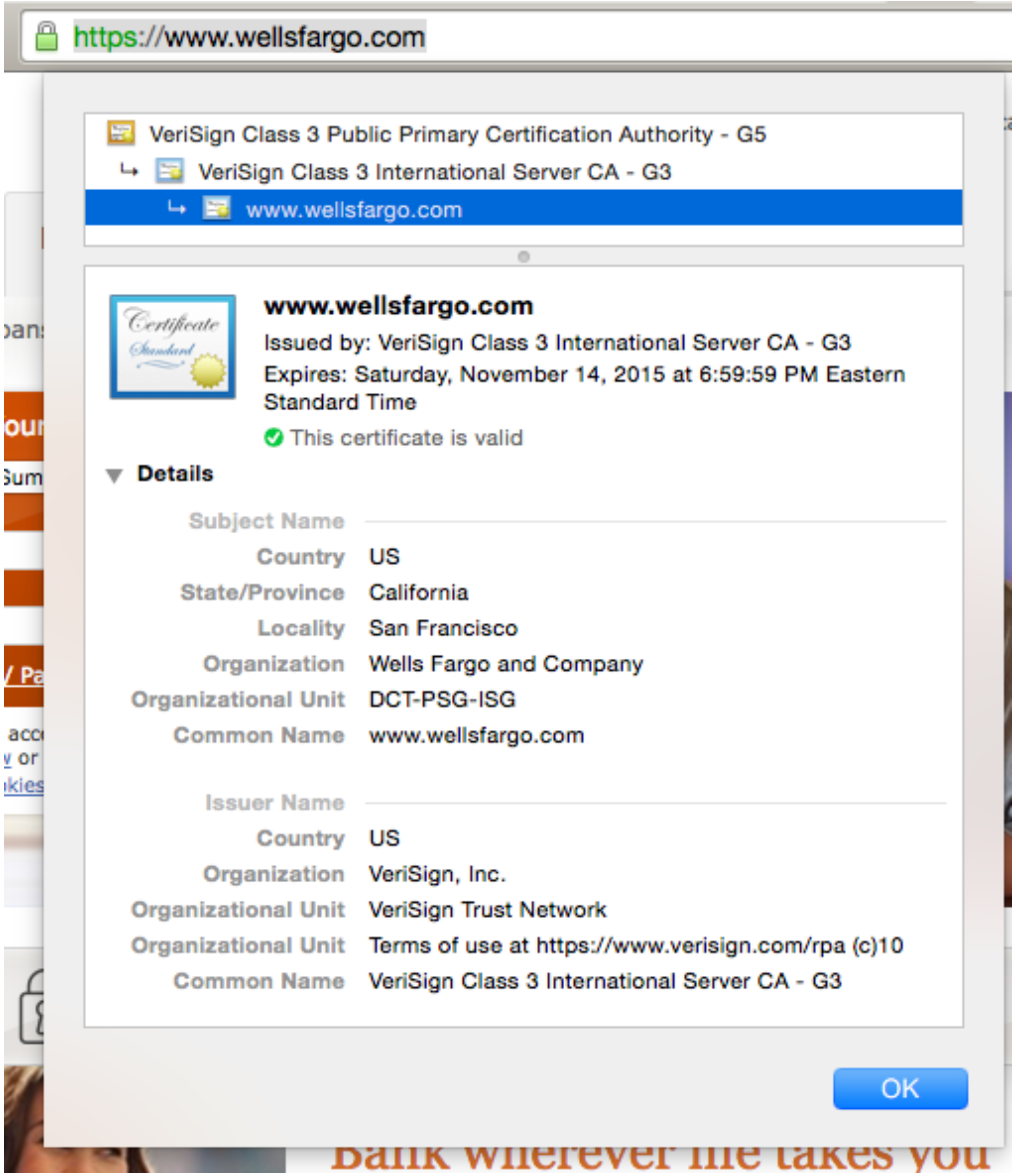
The connection uses TLS 1.2.

The connection is encrypted using RC4_128, with SHA1 for message authentication and RSA as the key exchange mechanism.

Site information

You first visited this site on Jan 18, 2015.

What do these mean?



https://www.wellsfargo.com

- VeriSign Class 3 Public Primary Certification Authority - G5
  - VeriSign Class 3 International Server CA - G3
    - www.wellsfargo.com

www.wellsfargo.com
Issued by: VeriSign Class 3 International Server CA - G3
Expires: Saturday, November 14, 2015 at 6:59:59 PM Eastern Standard Time
✓ This certificate is valid

▼ **Details**

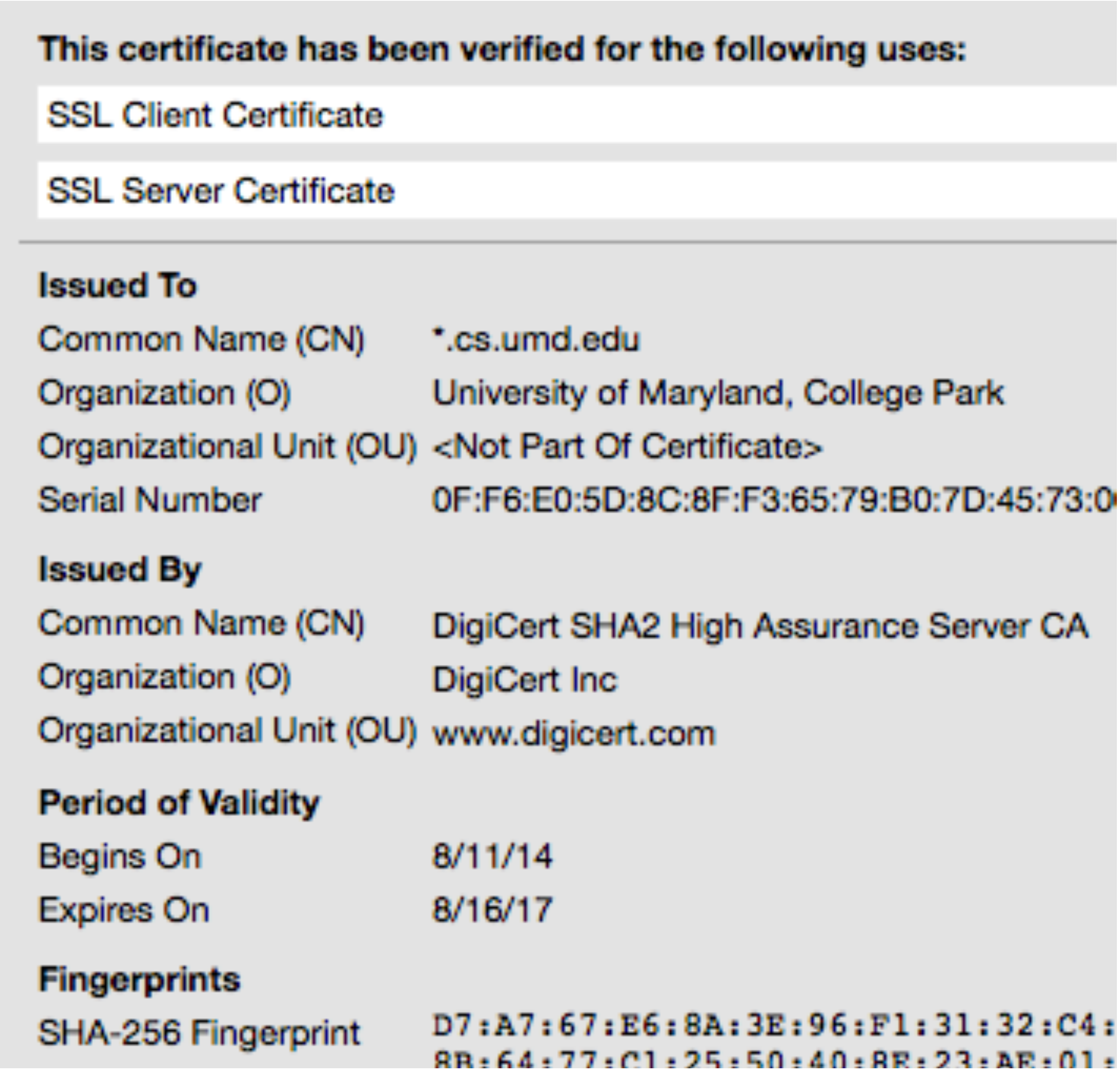
Subject Name	
Country	US
State/Province	California
Locality	San Francisco
Organization	Wells Fargo and Company
Organizational Unit	DCT-PSG-ISG
Common Name	www.wellsfargo.com
Issuer Name	
Country	US
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)10
Common Name	VeriSign Class 3 International Server CA - G3

Certificate chain

Subject (who owns the public key)

Common name: the URL of the subject

Issuer (who verified the identity and signed this certificate)



This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)	*.cs.umd.edu
Organization (O)	University of Maryland, College Park
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	0F:F6:E0:5D:8C:8F:F3:65:79:B0:7D:45:73:0

Issued By

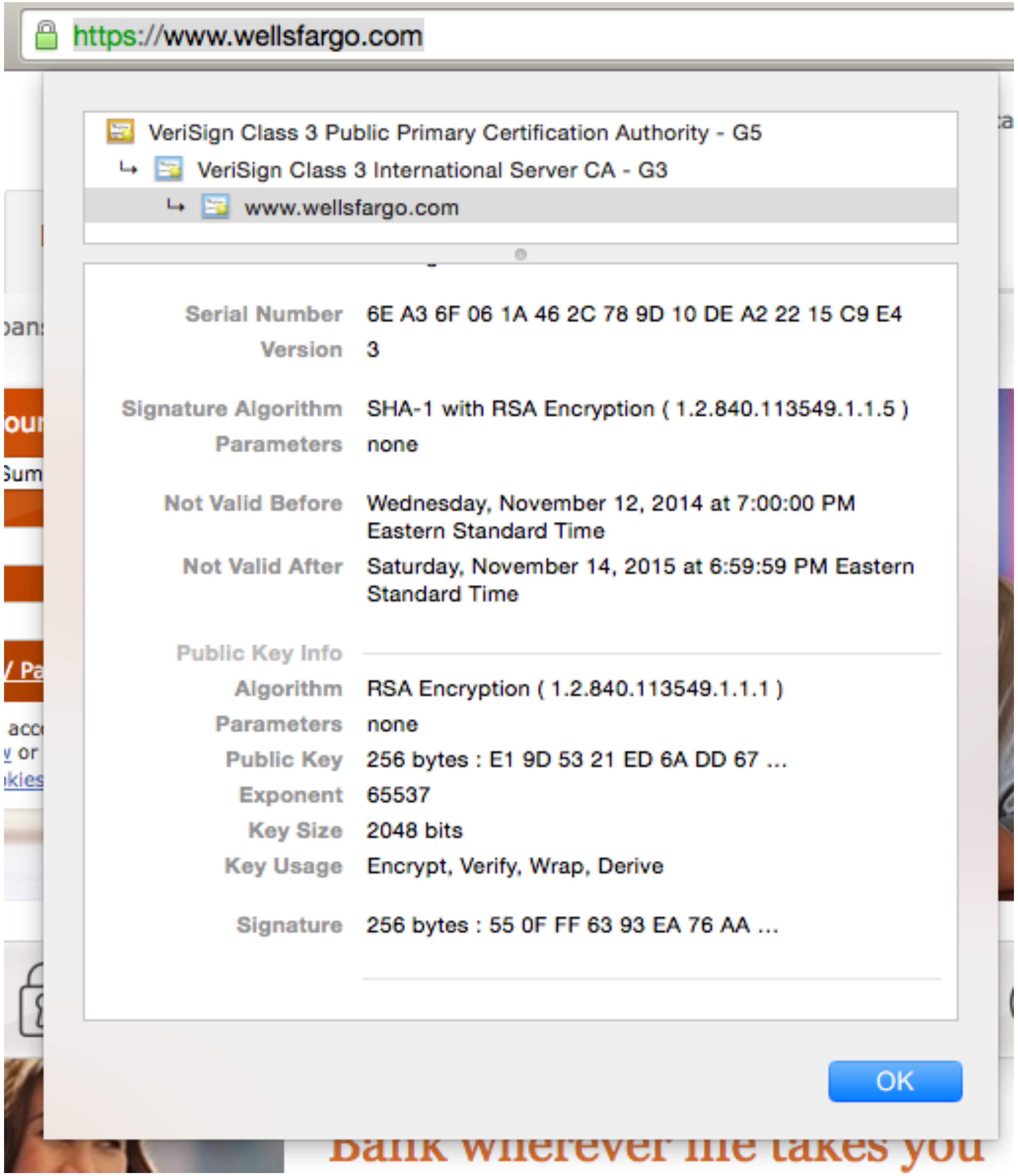
Common Name (CN)	DigiCert SHA2 High Assurance Server CA
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

Period of Validity

Begins On	8/11/14
Expires On	8/16/17

Fingerprints

SHA-256 Fingerprint	D7:A7:67:E6:8A:3E:96:F1:31:32:C4: 8B:64:77:C1:25:50:40:8E:23:AE:01:



https://www.wellsfargo.com

VeriSign Class 3 Public Primary Certification Authority - G5
↳ VeriSign Class 3 International Server CA - G3
↳ www.wellsfargo.com

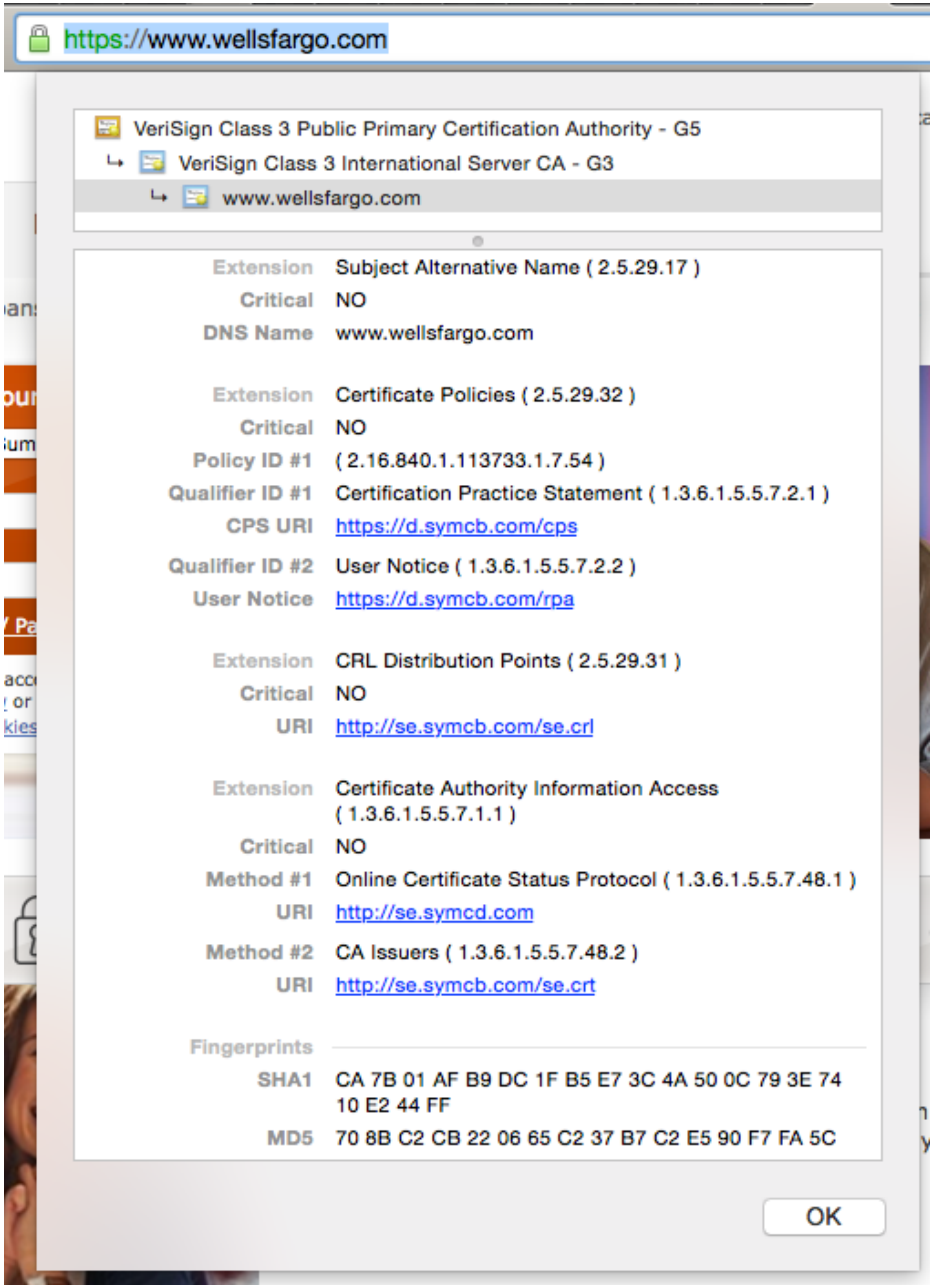
Serial Number	6E A3 6F 06 1A 46 2C 78 9D 10 DE A2 22 15 C9 E4
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Wednesday, November 12, 2014 at 7:00:00 PM Eastern Standard Time
Not Valid After	Saturday, November 14, 2015 at 6:59:59 PM Eastern Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : E1 9D 53 21 ED 6A DD 67 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	256 bytes : 55 0F FF 63 93 EA 76 AA ...

Serial number: Uniquely identifies this cert with respect to the issuer (look for this in CRLs)

Signature algorithm: How the issuer will sign parts of the cert

Not valid before/after: When to start and stop believing this cert (start & expiration dates)

The public key: And the issuer's signature of the public key



https://www.wellsfargo.com

VeriSign Class 3 Public Primary Certification Authority - G5
↳ VeriSign Class 3 International Server CA - G3
↳ www.wellsfargo.com

Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.wellsfargo.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(2.16.840.1.113733.1.7.54)
Qualifier ID #1	Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI	https://d.symcb.com/cps
Qualifier ID #2	User Notice (1.3.6.1.5.5.7.2.2)
User Notice	https://d.symcb.com/rpa
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://se.symcb.com/se.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://se.symcd.com
Method #2	CA Issuers (1.3.6.1.5.5.7.48.2)
URI	http://se.symcb.com/se.crt
Fingerprints	
SHA1	CA 7B 01 AF B9 DC 1F B5 E7 3C 4A 50 0C 79 3E 74 10 E2 44 FF
MD5	70 8B C2 CB 22 06 65 C2 37 B7 C2 E5 90 F7 FA 5C

Subject Alternate Names:
Other URLs for which this cert should be considered valid. (wellsfargo.com is not the same as www.wellsfargo.com)

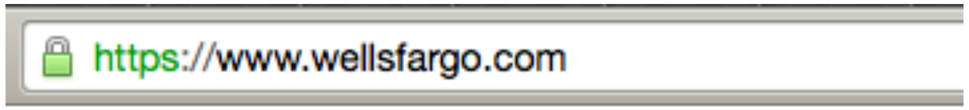
Can include wildcards, e.g., *.google.com

CRL & OCSP:
Where to go to check if this certificate has been revoked

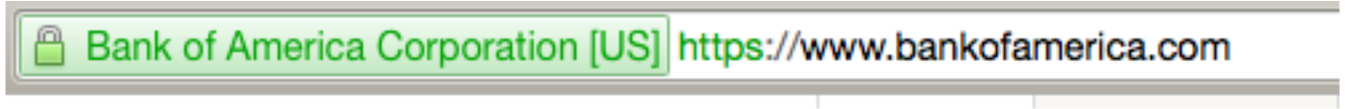
Non-cryptographic checksums

Certificate types

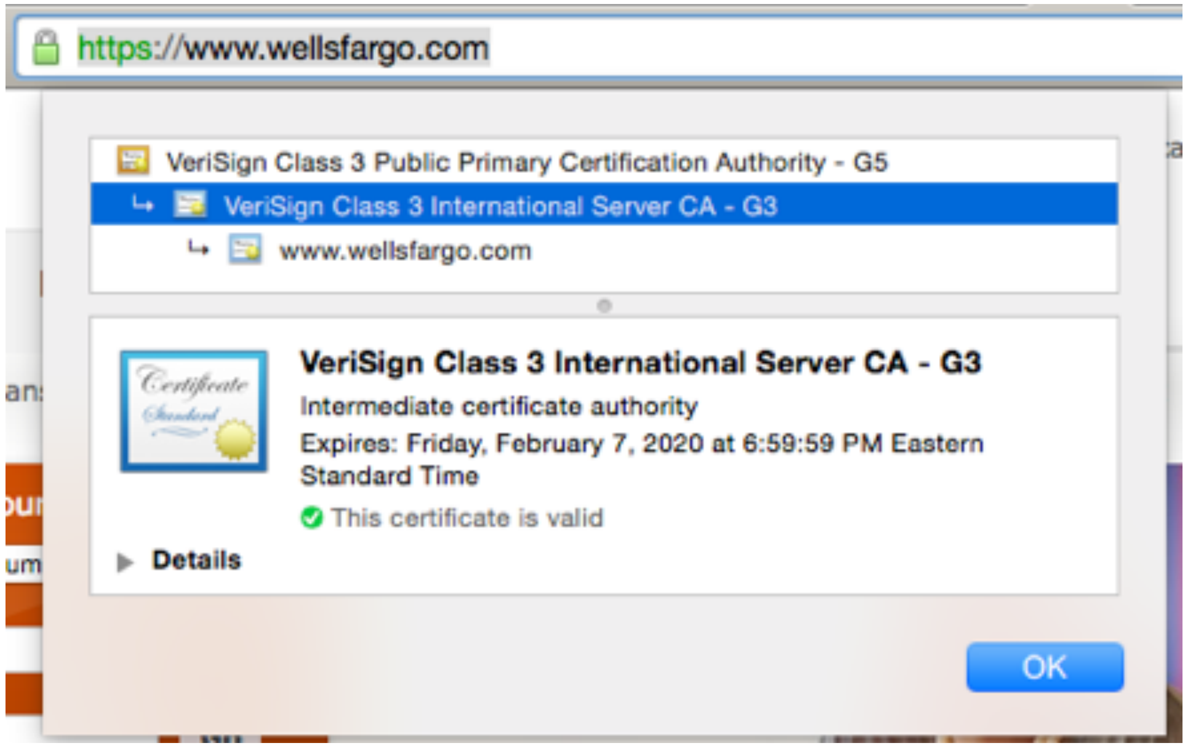
Why are these different?



https://www.wellsfargo.com



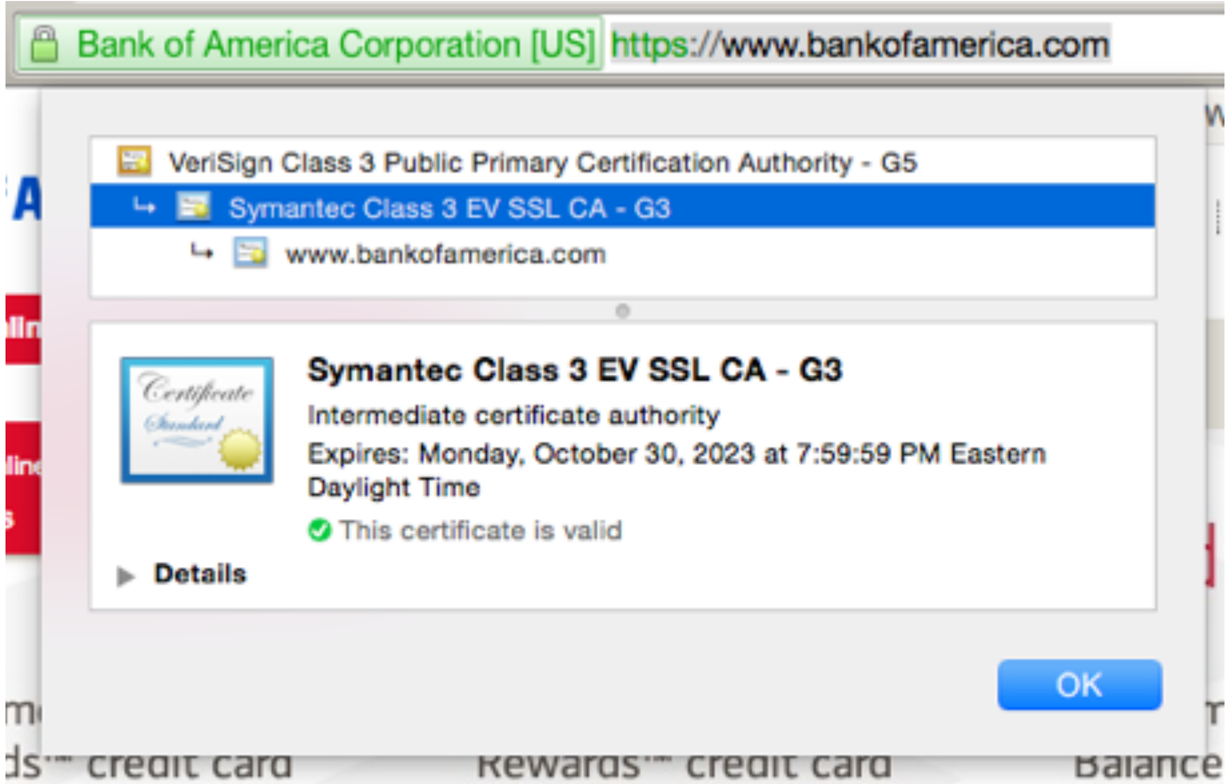
Bank of America Corporation [US] https://www.bankofamerica.com



https://www.wellsfargo.com

VeriSign Class 3 Public Primary Certification Authority - G5
↳ VeriSign Class 3 International Server CA - G3
↳ www.wellsfargo.com

VeriSign Class 3 International Server CA - G3
Intermediate certificate authority
Expires: Friday, February 7, 2020 at 6:59:59 PM Eastern Standard Time
✓ This certificate is valid



Bank of America Corporation [US] https://www.bankofamerica.com

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

Symantec Class 3 EV SSL CA - G3
Intermediate certificate authority
Expires: Monday, October 30, 2023 at 7:59:59 PM Eastern Daylight Time
✓ This certificate is valid

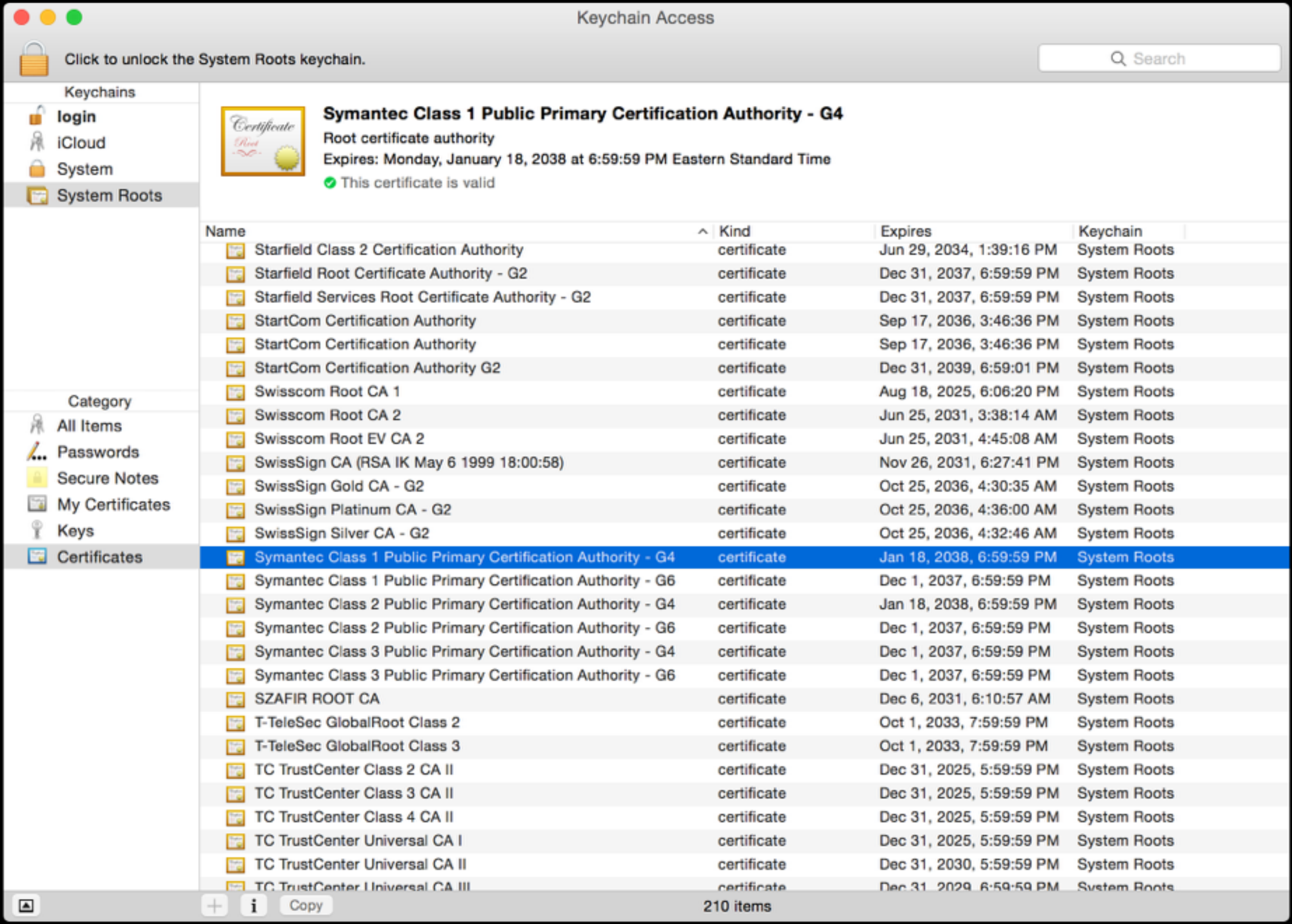
This is an EV (extended validation) certificate; browsers show the full name for these kinds of certs

Root CAs

Root CAs in iOS9

- iOS9 ships with >50 that start with A-C
- Full list at:
  https://support.apple.com/en-us/HT205205

Verifying certificates



Click to unlock the System Roots keychain.

Symantec Class 1 Public Primary Certification Authority - G4

Root certificate authority

Expires: Monday, January 18, 2038 at 6:59:59 PM Eastern Standard Time

✓ This certificate is valid

Name	Kind	Expires	Keychain
Starfield Class 2 Certification Authority	certificate	Jun 29, 2034, 1:39:16 PM	System Roots
Starfield Root Certificate Authority - G2	certificate	Dec 31, 2037, 6:59:59 PM	System Roots
Starfield Services Root Certificate Authority - G2	certificate	Dec 31, 2037, 6:59:59 PM	System Roots
StartCom Certification Authority	certificate	Sep 17, 2036, 3:46:36 PM	System Roots
StartCom Certification Authority	certificate	Sep 17, 2036, 3:46:36 PM	System Roots
StartCom Certification Authority G2	certificate	Dec 31, 2039, 6:59:01 PM	System Roots
Swisscom Root CA 1	certificate	Aug 18, 2025, 6:06:20 PM	System Roots
Swisscom Root CA 2	certificate	Jun 25, 2031, 3:38:14 AM	System Roots
Swisscom Root EV CA 2	certificate	Jun 25, 2031, 4:45:08 AM	System Roots
SwissSign CA (RSA IK May 6 1999 18:00:58)	certificate	Nov 26, 2031, 6:27:41 PM	System Roots
SwissSign Gold CA - G2	certificate	Oct 25, 2036, 4:30:35 AM	System Roots
SwissSign Platinum CA - G2	certificate	Oct 25, 2036, 4:36:00 AM	System Roots
SwissSign Silver CA - G2	certificate	Oct 25, 2036, 4:32:46 AM	System Roots
Symantec Class 1 Public Primary Certification Authority - G4	certificate	Jan 18, 2038, 6:59:59 PM	System Roots
Symantec Class 1 Public Primary Certification Authority - G6	certificate	Dec 1, 2037, 6:59:59 PM	System Roots
Symantec Class 2 Public Primary Certification Authority - G4	certificate	Jan 18, 2038, 6:59:59 PM	System Roots
Symantec Class 2 Public Primary Certification Authority - G6	certificate	Dec 1, 2037, 6:59:59 PM	System Roots
Symantec Class 3 Public Primary Certification Authority - G4	certificate	Dec 1, 2037, 6:59:59 PM	System Roots
Symantec Class 3 Public Primary Certification Authority - G6	certificate	Dec 1, 2037, 6:59:59 PM	System Roots
SZAFIR ROOT CA	certificate	Dec 6, 2031, 6:10:57 AM	System Roots
T-TeleSec GlobalRoot Class 2	certificate	Oct 1, 2033, 7:59:59 PM	System Roots
T-TeleSec GlobalRoot Class 3	certificate	Oct 1, 2033, 7:59:59 PM	System Roots
TC TrustCenter Class 2 CA II	certificate	Dec 31, 2025, 5:59:59 PM	System Roots
TC TrustCenter Class 3 CA II	certificate	Dec 31, 2025, 5:59:59 PM	System Roots
TC TrustCenter Class 4 CA II	certificate	Dec 31, 2025, 5:59:59 PM	System Roots
TC TrustCenter Universal CA I	certificate	Dec 31, 2025, 5:59:59 PM	System Roots
TC TrustCenter Universal CA II	certificate	Dec 31, 2030, 5:59:59 PM	System Roots
TC TrustCenter Universal CA III	certificate	Dec 31, 2029, 6:59:59 PM	System Roots

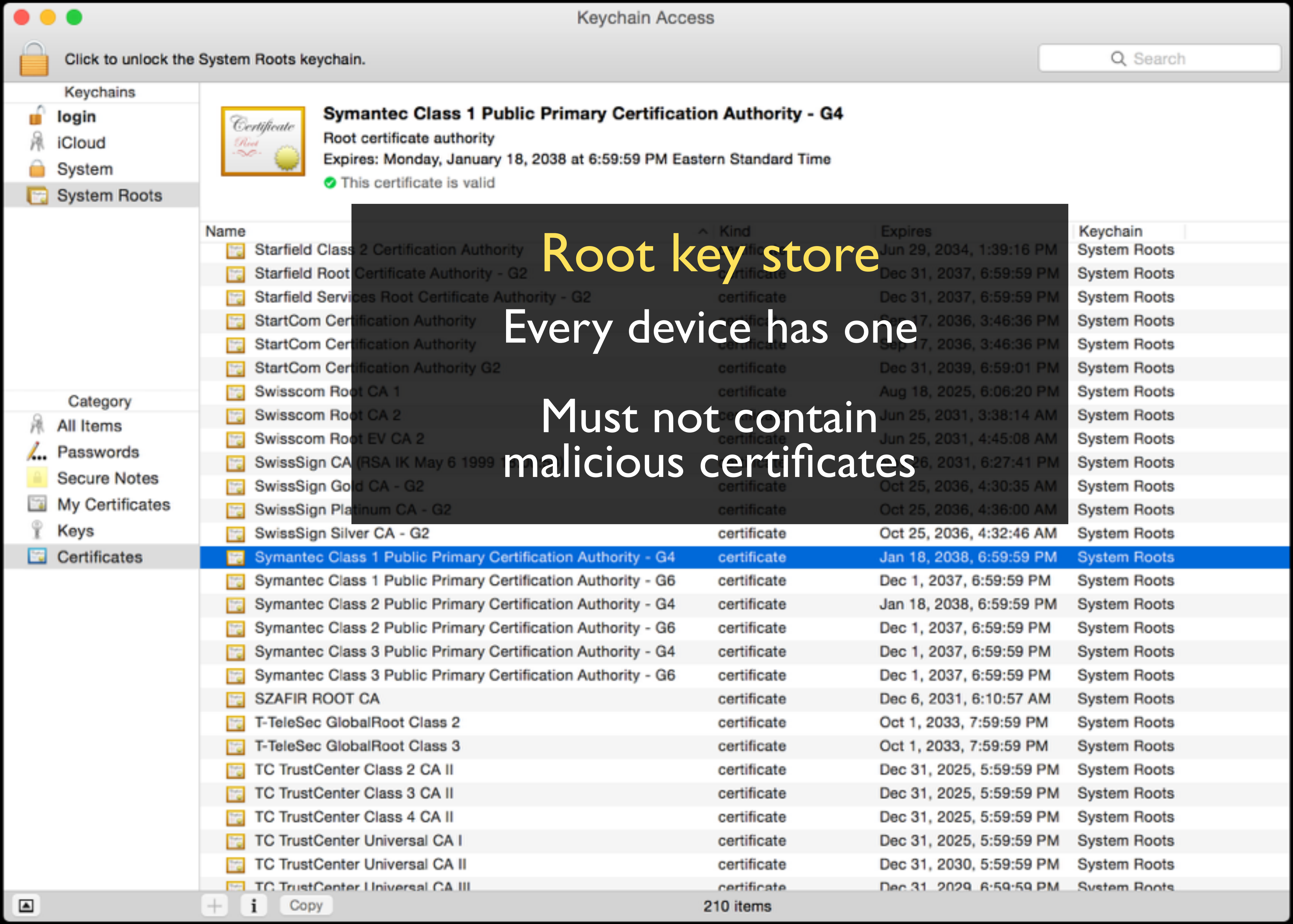
210 items

Verifying certificates

Root key store

Every device has one

Must not contain malicious certificates



Click to unlock the System Roots keychain.

Symantec Class 1 Public Primary Certification Authority - G4
Root certificate authority
Expires: Monday, January 18, 2038 at 6:59:59 PM Eastern Standard Time
✓ This certificate is valid

Name	Kind	Expires	Keychain
Starfield Class 2 Certification Authority	certificate	Jun 29, 2034, 1:39:16 PM	System Roots
Starfield Root Certificate Authority - G2	certificate	Dec 31, 2037, 6:59:59 PM	System Roots
Starfield Services Root Certificate Authority - G2	certificate	Dec 31, 2037, 6:59:59 PM	System Roots
StartCom Certification Authority	certificate	Sep 17, 2036, 3:46:36 PM	System Roots
StartCom Certification Authority	certificate	Sep 17, 2036, 3:46:36 PM	System Roots
StartCom Certification Authority G2	certificate	Dec 31, 2039, 6:59:01 PM	System Roots
Swisscom Root CA 1	certificate	Aug 18, 2025, 6:06:20 PM	System Roots
Swisscom Root CA 2	certificate	Jun 25, 2031, 3:38:14 AM	System Roots
Swisscom Root EV CA 2	certificate	Jun 25, 2031, 4:45:08 AM	System Roots
SwissSign CA (RSA IK May 6 1999 [illegible]	certificate	[illegible] 26, 2031, 6:27:41 PM	System Roots
SwissSign Gold CA - G2	certificate	Oct 25, 2036, 4:30:35 AM	System Roots
SwissSign Platinum CA - G2	certificate	Oct 25, 2036, 4:36:00 AM	System Roots
SwissSign Silver CA - G2	certificate	Oct 25, 2036, 4:32:46 AM	System Roots
Symantec Class 1 Public Primary Certification Authority - G4	certificate	Jan 18, 2038, 6:59:59 PM	System Roots
Symantec Class 1 Public Primary Certification Authority - G6	certificate	Dec 1, 2037, 6:59:59 PM	System Roots
Symantec Class 2 Public Primary Certification Authority - G4	certificate	Jan 18, 2038, 6:59:59 PM	System Roots
Symantec Class 2 Public Primary Certification Authority - G6	certificate	Dec 1, 2037, 6:59:59 PM	System Roots
Symantec Class 3 Public Primary Certification Authority - G4	certificate	Dec 1, 2037, 6:59:59 PM	System Roots
Symantec Class 3 Public Primary Certification Authority - G6	certificate	Dec 1, 2037, 6:59:59 PM	System Roots
SZAFIR ROOT CA	certificate	Dec 6, 2031, 6:10:57 AM	System Roots
T-TeleSec GlobalRoot Class 2	certificate	Oct 1, 2033, 7:59:59 PM	System Roots
T-TeleSec GlobalRoot Class 3	certificate	Oct 1, 2033, 7:59:59 PM	System Roots
TC TrustCenter Class 2 CA II	certificate	Dec 31, 2025, 5:59:59 PM	System Roots
TC TrustCenter Class 3 CA II	certificate	Dec 31, 2025, 5:59:59 PM	System Roots
TC TrustCenter Class 4 CA II	certificate	Dec 31, 2025, 5:59:59 PM	System Roots
TC TrustCenter Universal CA I	certificate	Dec 31, 2025, 5:59:59 PM	System Roots
TC TrustCenter Universal CA II	certificate	Dec 31, 2030, 5:59:59 PM	System Roots
TC TrustCenter Universal CA III	certificate	Dec 31, 2029, 6:59:59 PM	System Roots

CA compromise

- 2001: Verisign issued two code-signing certificates for Microsoft Corporation
  - To someone who ***didn't actually*** work at MS
  - No functional revocation paradigm
- 2011: Signing keys compromised at Comodo and DigiNotar
  - Bad certs for Google, Yahoo!, Tor, others
  - Seem to have been used mostly in Iran
- Some CAs are less picky than others

Case study: Superfish (Feb 2015)

- Lenovo laptops shipped with “Superfish” adware
- Installs self-signed root cert into browsers
  - MITM on every HTTPS site to inject ads
- Worse: Same private key for every laptop
  - Password = “komodia” (company
- ***Lenovo“did not find any evidence to substantiate security concerns”***

http://www.sainteldaily.com/archives/11400

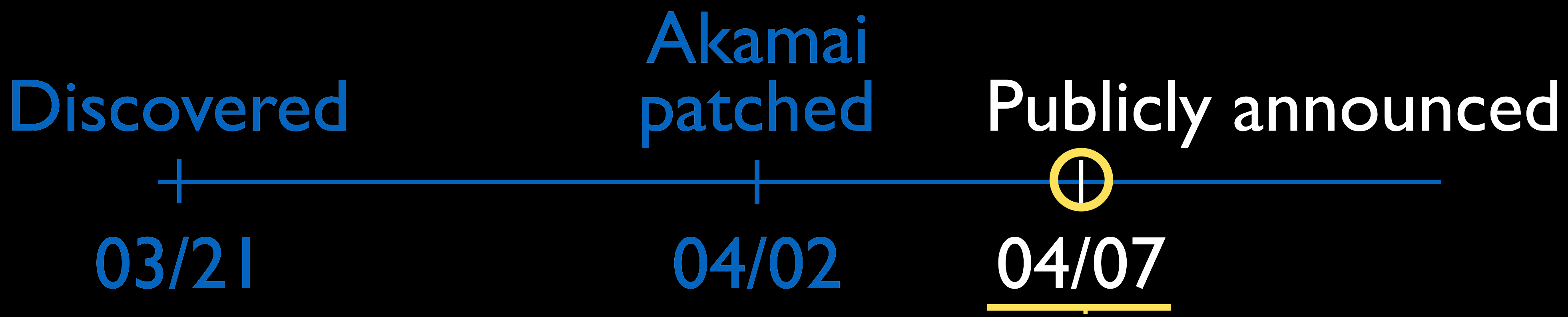
http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/

Heartbleed and Revocation

Remember Heartbleed (2014)

- OpenSSL vulnerability
- Discovered 03/21 Public 04/07
- Potential compromise
  - 100ks hosts
  - 20M total certs
  - 1.5M certs for Alexa top 1M domains
  - 600k leaf certs
  - 165k domains
- Correct procedure: patch, revoke, reissue

Why study Heartbleed?



Discovered 03/21

Akamai patched 04/02

Publicly announced 04/07

Every vulnerable website should have:

1 Patched

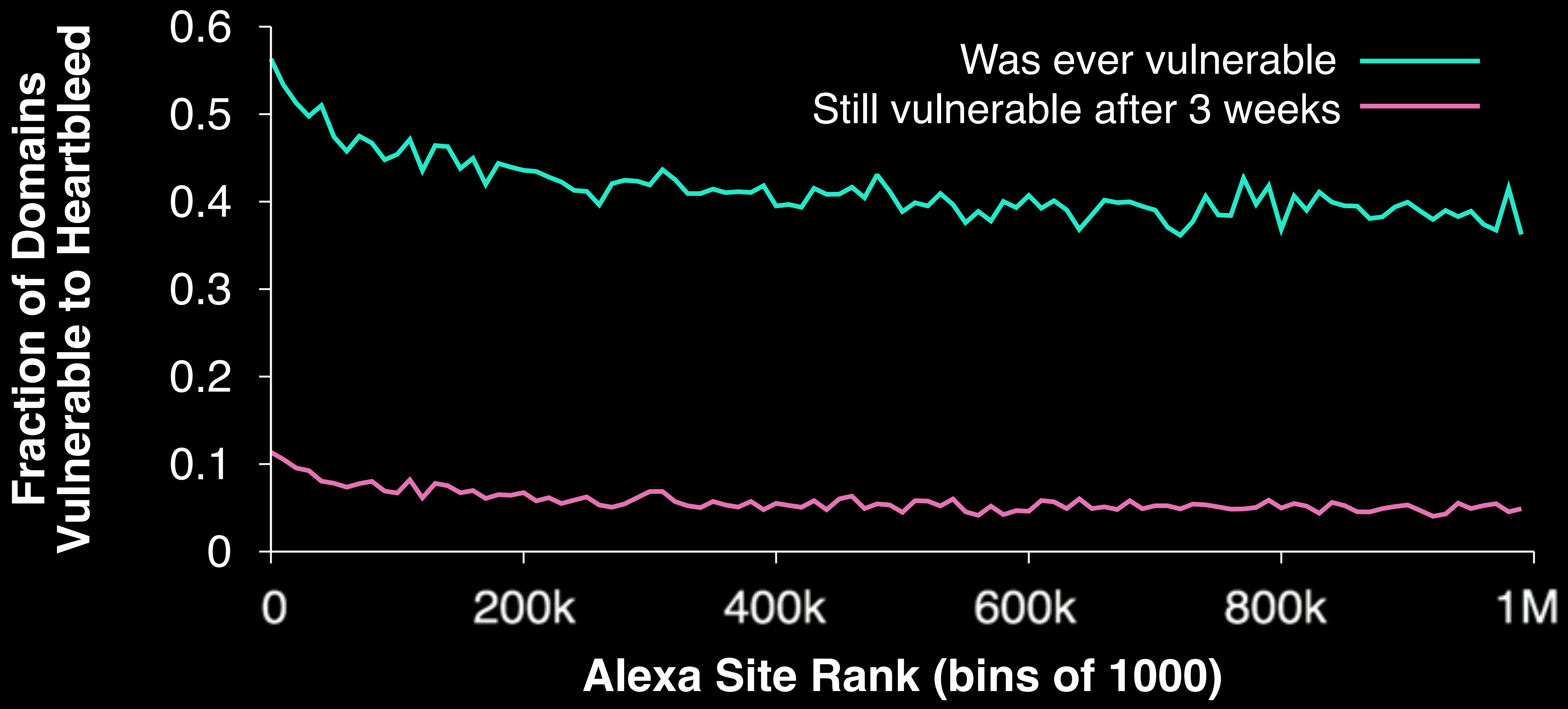
2 Revoked

3 Reissued

Heartbleed is a natural experiment:

How quickly and thoroughly do administrators act?

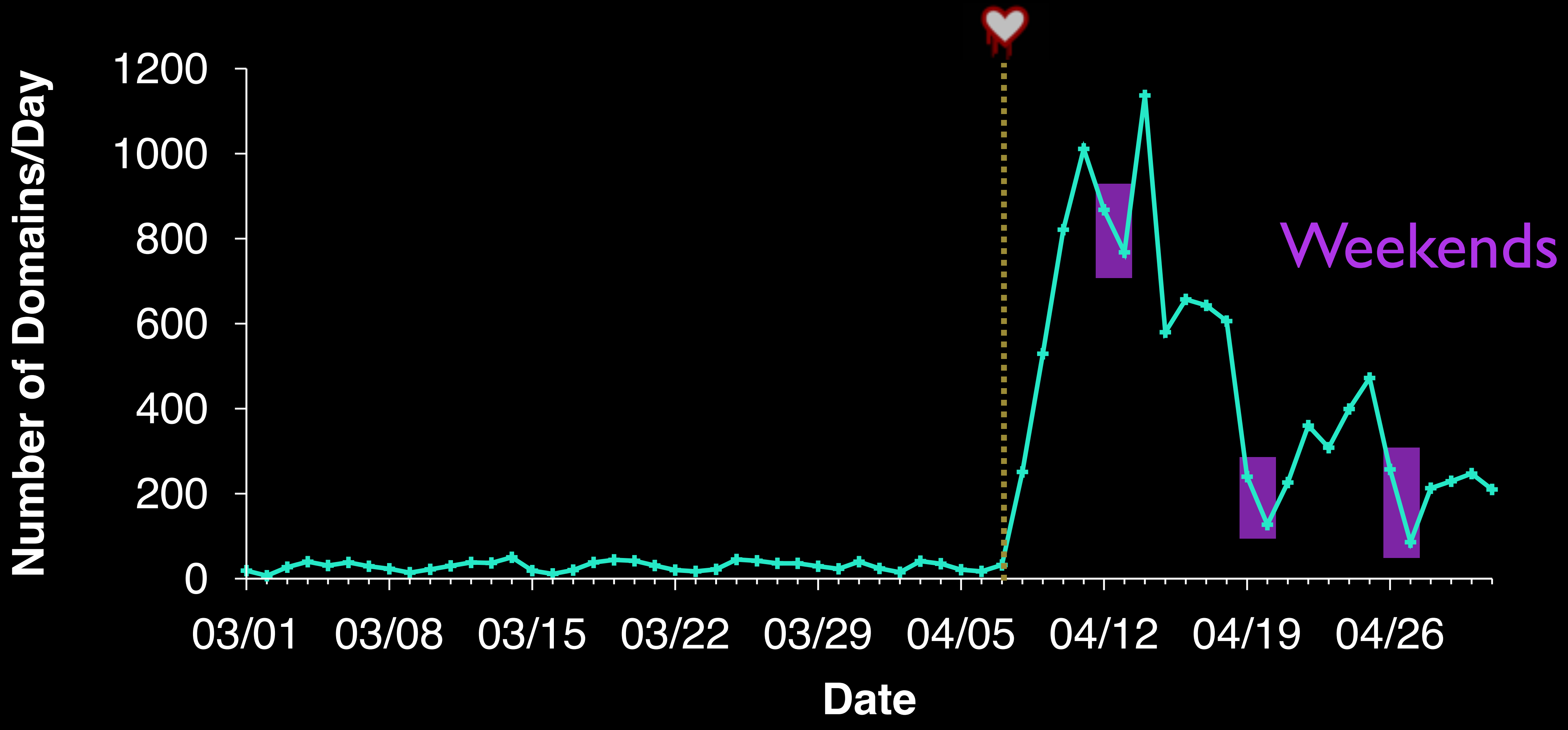
Prevalence and patch rates



Patching rates are mostly positive

Only ~7% had not patched within 3 weeks

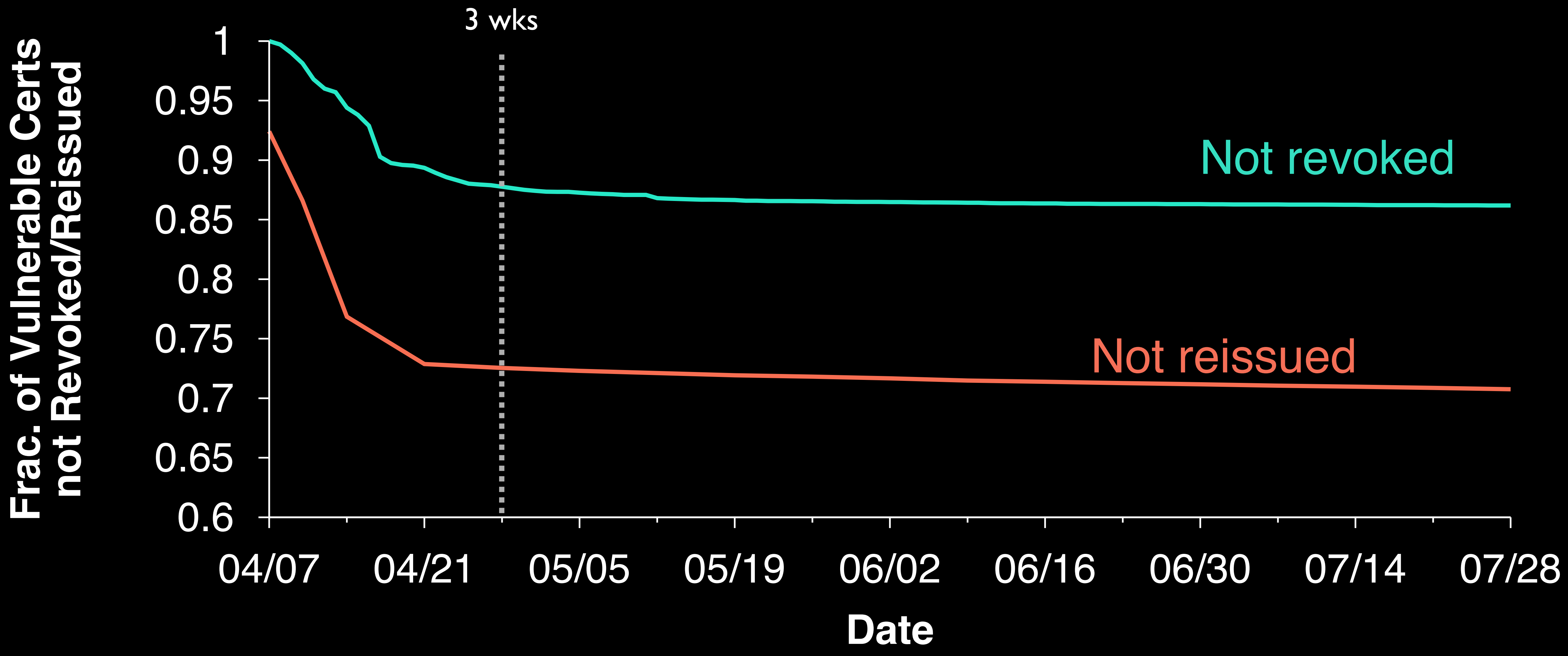
How quickly were certs revoked?



Reaction ramps up quickly

Security takes the weekends off

Certificate update rates

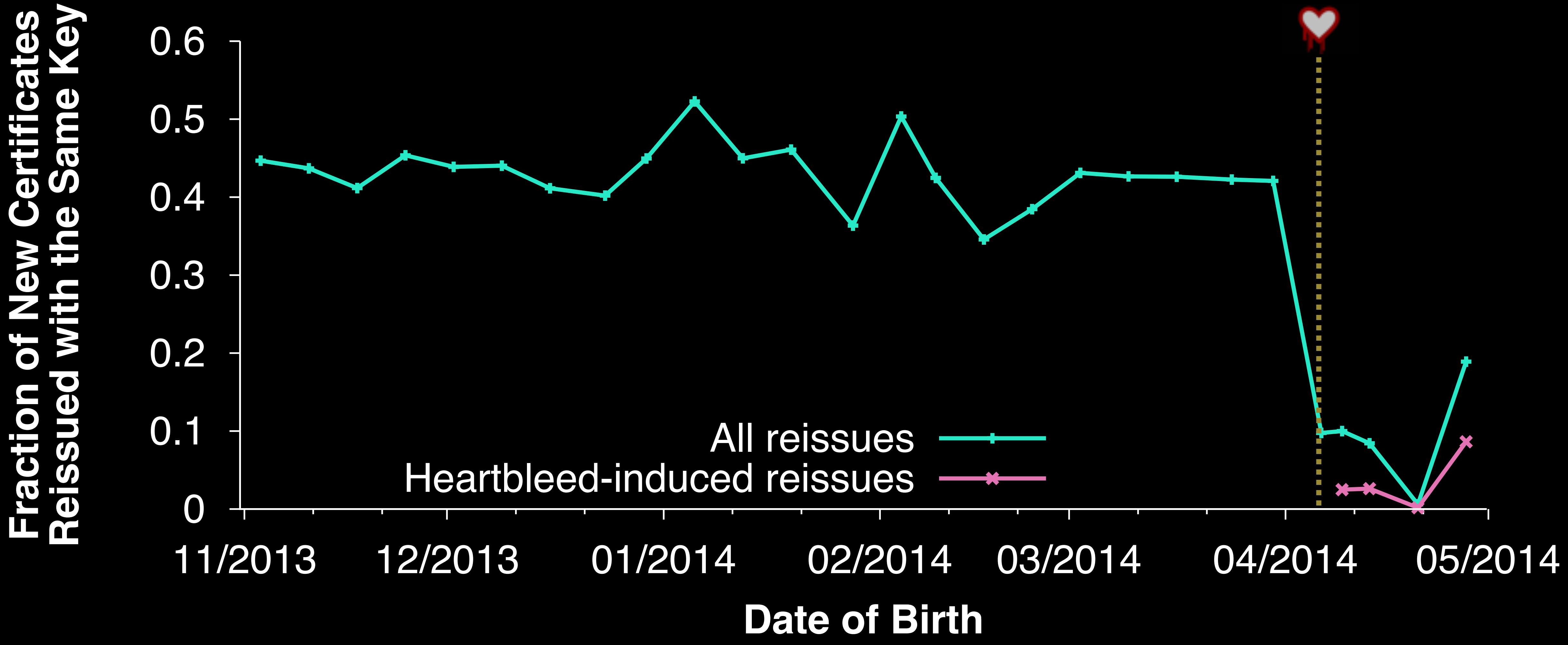


Similar pattern to patches:

Exponential drop-off, then levels out

After 3 weeks: 13% Revoked 27% Reissued

Reissue ⇒ New key?



Reissuing the same key is common practice

4.1% Heartbleed-induced

The ugly truth of revocations

93% Patched

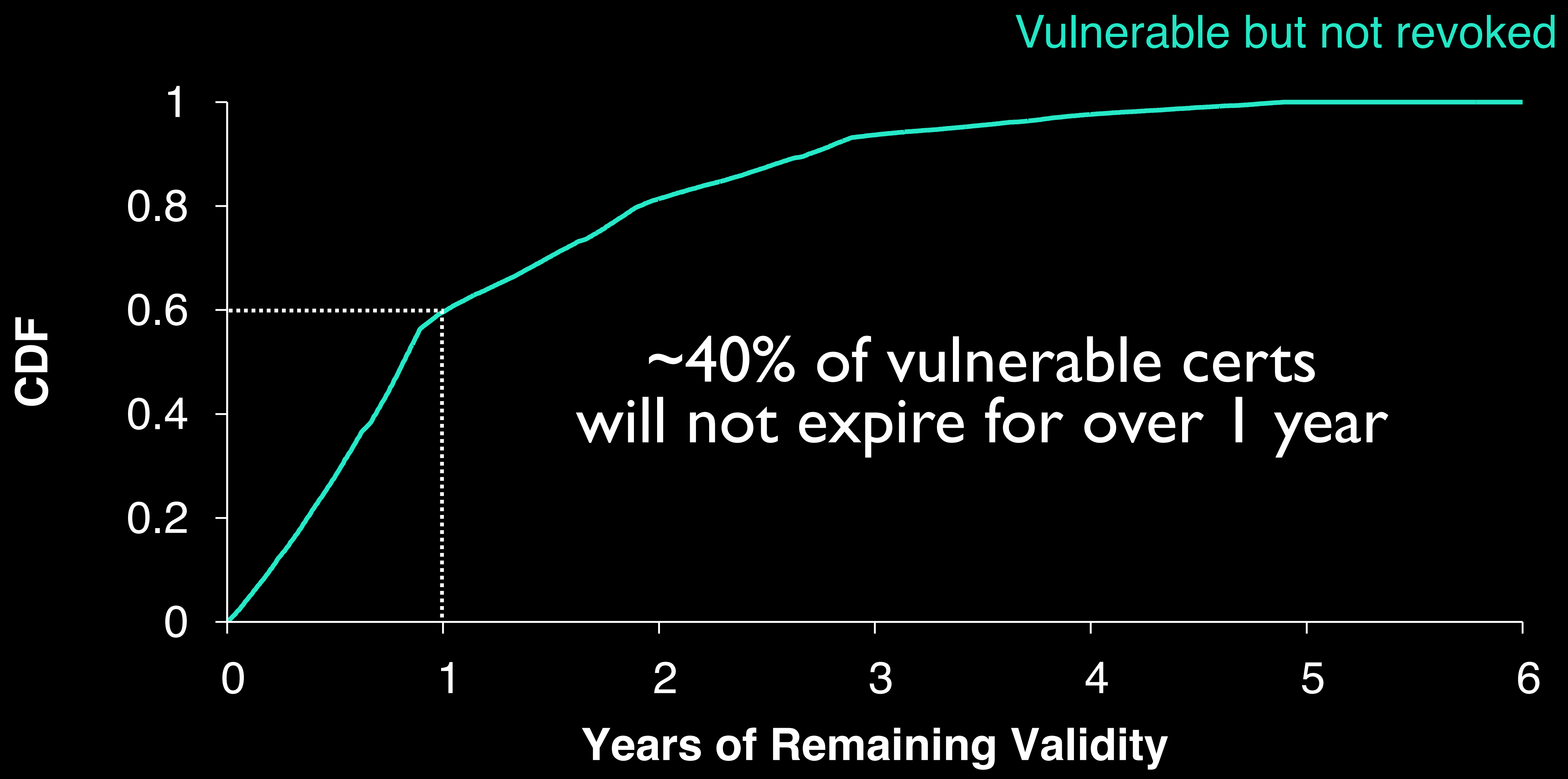
13% Revoked

27% Reissued

Security is supposed to be a fundamental design goal, but

- Administrators trade off security for *ease of maintenance/cost*
- Certificate authorities trade off security for *profit*

Can we wait for expiration?



~40% of vulnerable certs
will not expire for over 1 year

We may be dealing with Heartbleed for *years*

How well do browsers check certificates

Testing browser behavior

Revocation protocols

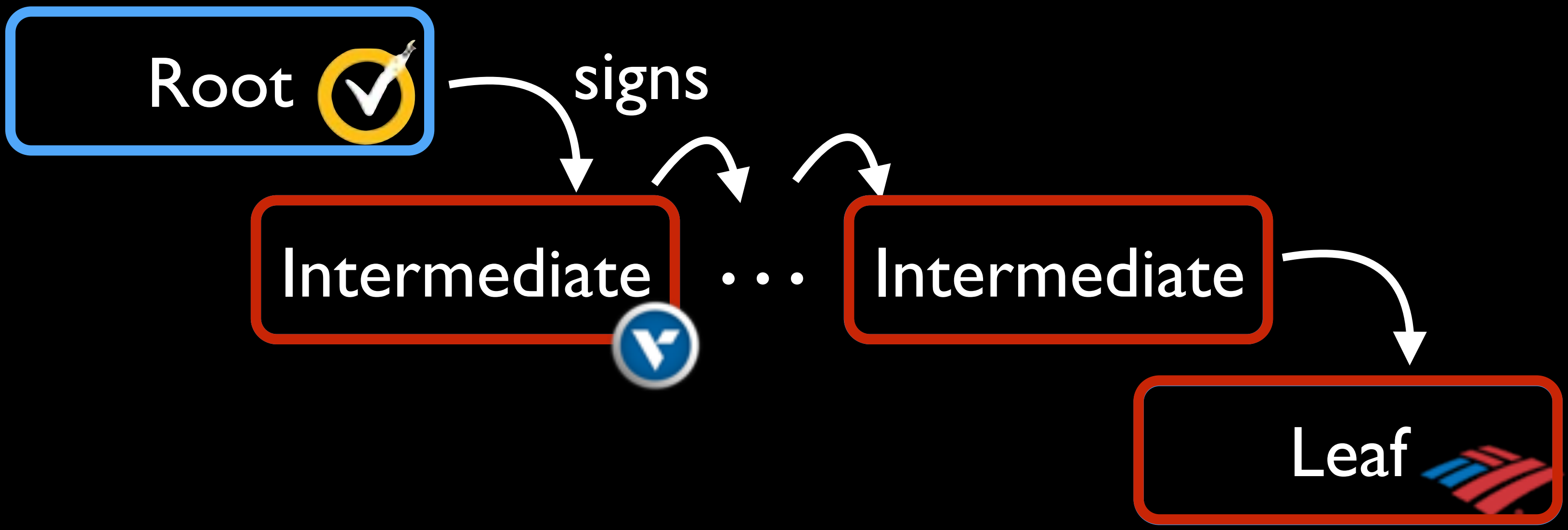
- Browsers *should* support all major protocols
  - CRLs, OCSP, OCSP stapling

Availability of revocation info

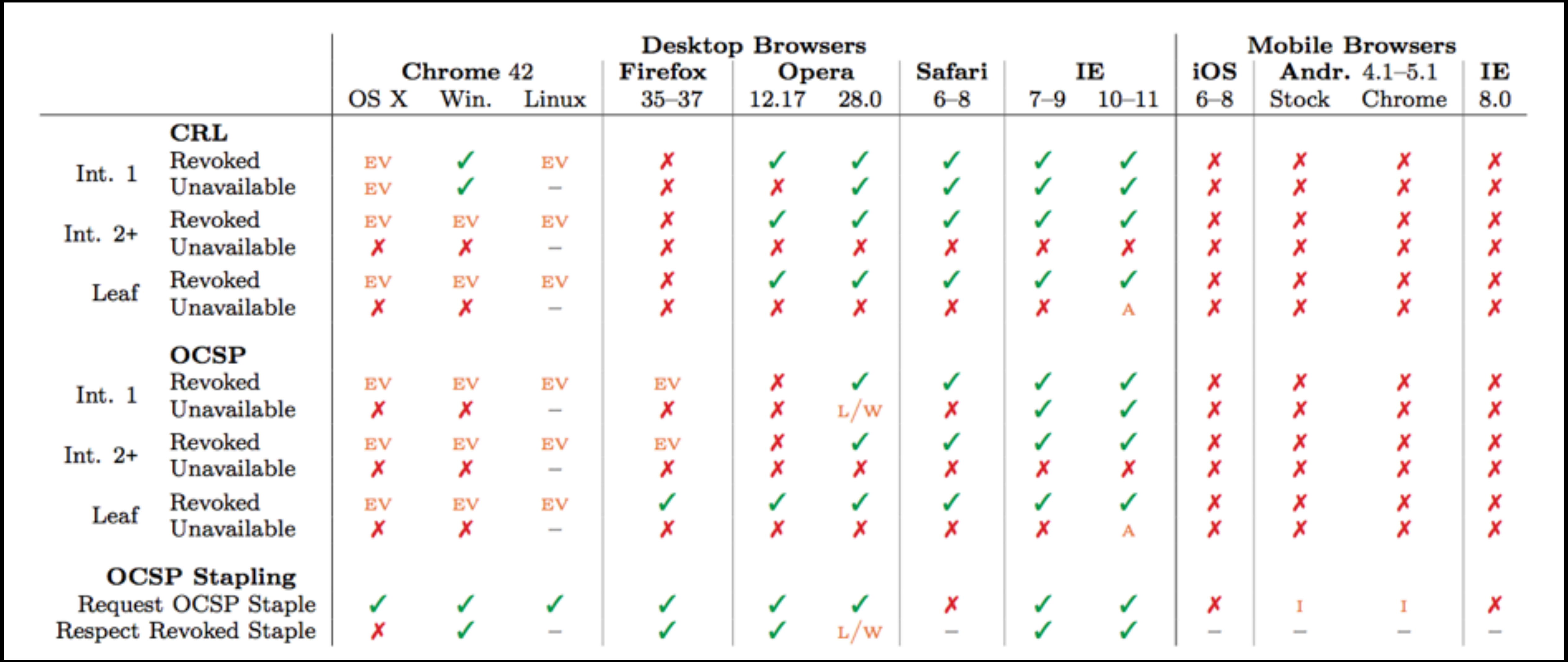
- Browsers *should* reject certs they cannot check
  - E.g., because the OCSP server is down

Chain lengths

- Browsers *should* reject a cert if *any* on the chain fail
  - Leaf, intermediate(s), root



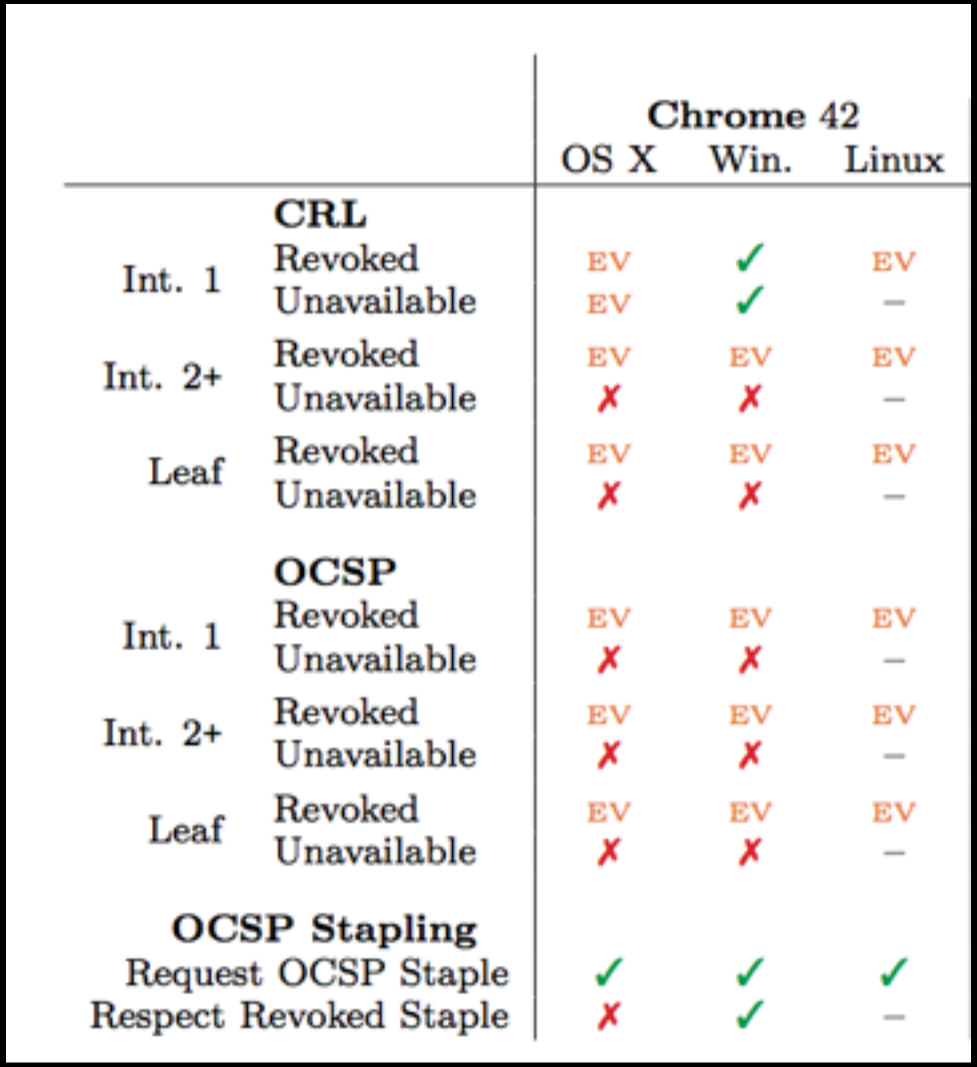
Results across all browsers



			Desktop Browsers								Mobile Browsers		
		Chrome 42			Firefox	Opera		Safari	IE		iOS	Andr. 4.1–5.1		IE
		OS X	Win.	Linux	35–37	12.17	28.0	6–8	7–9	10–11	6–8	Stock	Chrome	8.0
	CRL													
Int. 1	Revoked	EV	✓	EV	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	EV	✓	–	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
Int. 2+	Revoked	EV	EV	EV	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Leaf	Revoked	EV	EV	EV	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	✗	✗	✗	A	✗	✗	✗	✗
	OCSP													
Int. 1	Revoked	EV	EV	EV	EV	✗	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	L/W	✗	✓	✓	✗	✗	✗	✗
Int. 2+	Revoked	EV	EV	EV	EV	✗	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Leaf	Revoked	EV	EV	EV	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	✗	✗	✗	A	✗	✗	✗	✗
OCSP Stapling														
Request OCSP Staple		✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	I	I	✗
Respect Revoked Staple		✗	✓	–	✓	✓	L/W	–	✓	✓	–	–	–	–

✓ Passes test	**EV** Passes for EV certs	**A** Pops up alert to user
✗ Fails test	**I** Ignores OCSP Staple	**L/W** Passes on Linux/Win.

Results across all browsers



		Chrome 42		
		OS X	Win.	Linux
	CRL			
Int. 1	Revoked	EV	✓	EV
	Unavailable	EV	✓	–
Int. 2+	Revoked	EV	EV	EV
	Unavailable	✗	✗	–
Leaf	Revoked	EV	EV	EV
	Unavailable	✗	✗	–
	OCSP			
Int. 1	Revoked	EV	EV	EV
	Unavailable	✗	✗	–
Int. 2+	Revoked	EV	EV	EV
	Unavailable	✗	✗	–
Leaf	Revoked	EV	EV	EV
	Unavailable	✗	✗	–
OCSP Stapling				
Request OCSP Staple		✓	✓	✓
Respect Revoked Staple		✗	✓	–

Chrome

Generally, only checks for EV certs

~3% of all certs

Allows if revocation info unavailable

Supports OCSP stapling

✓ Passes test

✗ Fails test

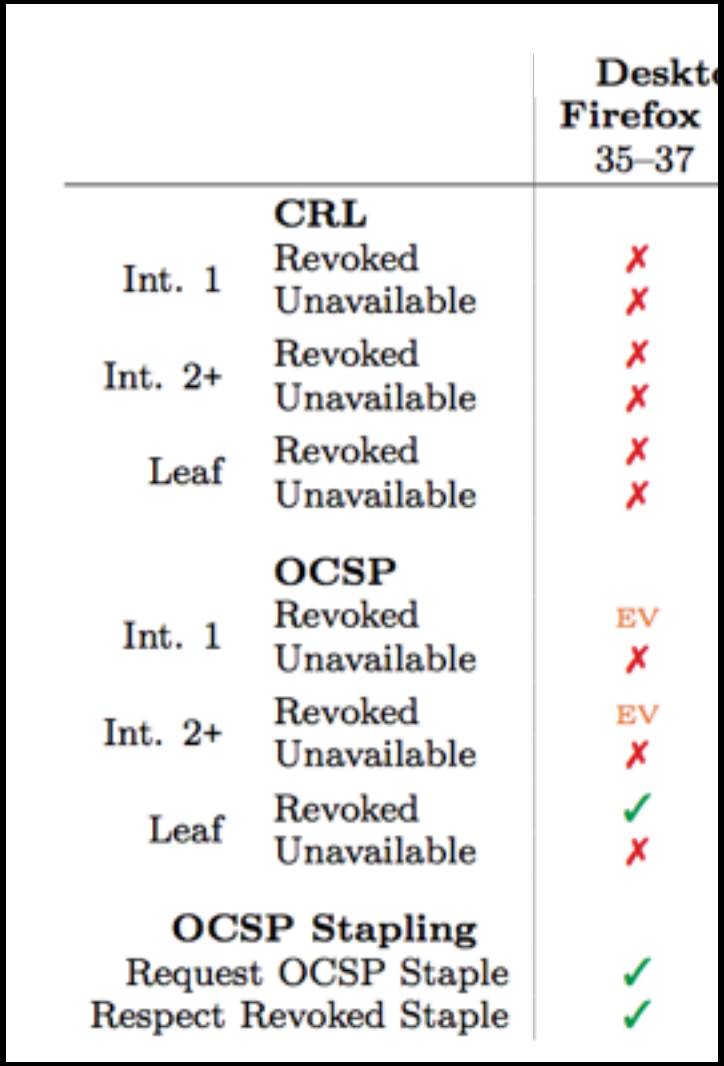
EV Passes for EV certs

I Ignores OCSP Staple

A Pops up alert to user

L/W Passes on Linux/Win.

Results across all browsers



		Deskt Firefox 35–37
	CRL	
Int. 1	Revoked	✗
	Unavailable	✗
Int. 2+	Revoked	✗
	Unavailable	✗
Leaf	Revoked	✗
	Unavailable	✗
	OCSP	
Int. 1	Revoked	EV
	Unavailable	✗
Int. 2+	Revoked	EV
	Unavailable	✗
Leaf	Revoked	✓
	Unavailable	✗
	OCSP Stapling	
	Request OCSP Staple	✓
	Respect Revoked Staple	✓

Firefox

Never checks CRLs

Only checks intermediates for EV certs

Allows if revocation info unavailable

Supports OCSP stapling

✓ Passes test

✗ Fails test

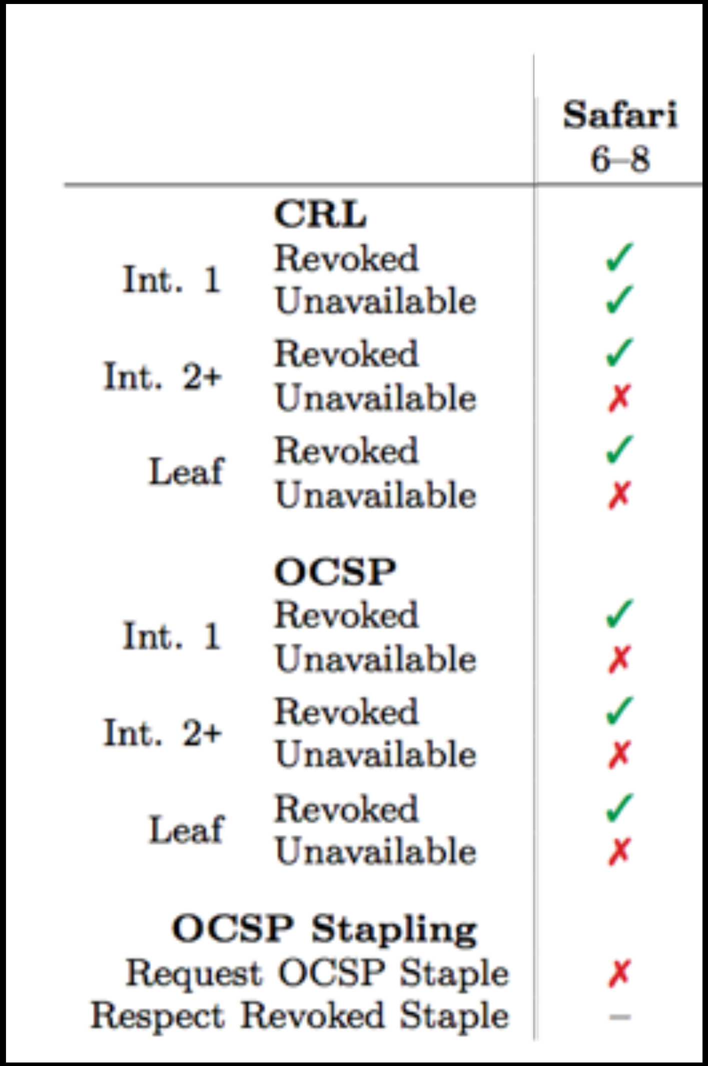
EV Passes for EV certs

I Ignores OCSP Staple

A Pops up alert to user

L/W Passes on Linux/Win.

Results across all browsers



		Safari 6–8
	CRL	
Int. 1	Revoked	✓
	Unavailable	✓
Int. 2+	Revoked	✓
	Unavailable	✗
Leaf	Revoked	✓
	Unavailable	✗
	OCSP	
Int. 1	Revoked	✓
	Unavailable	✗
Int. 2+	Revoked	✓
	Unavailable	✗
Leaf	Revoked	✓
	Unavailable	✗
OCSP Stapling		
Request OCSP Staple		✗
Respect Revoked Staple		–

Safari

Checks CRLs and OCSP

Allows if revocation info unavailable

Except for first intermediate, for CRLs

Does *not* support OCSP stapling

✓ Passes test

✗ Fails test

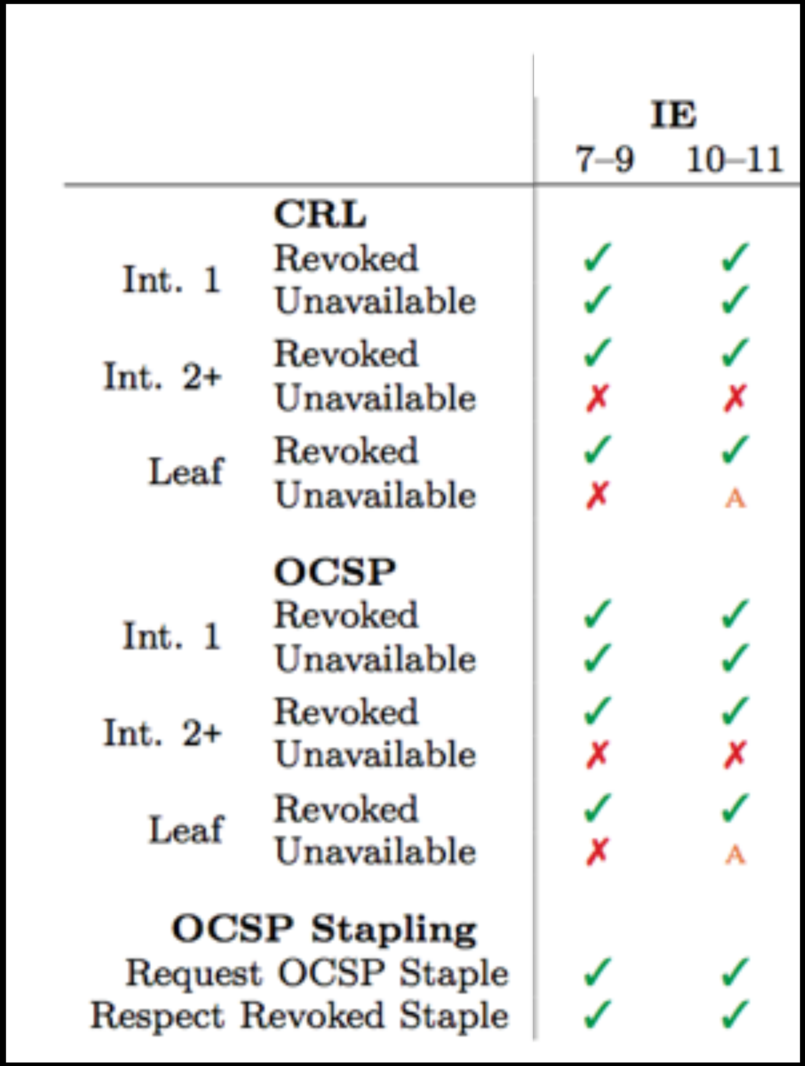
EV Passes for EV certs

I Ignores OCSP Staple

A Pops up alert to user

L/W Passes on Linux/Win.

Results across all browsers



		IE	
		7–9	10–11
	CRL		
Int. 1	Revoked	✓	✓
	Unavailable	✓	✓
Int. 2+	Revoked	✓	✓
	Unavailable	✗	✗
Leaf	Revoked	✓	✓
	Unavailable	✗	A
	OCSP		
Int. 1	Revoked	✓	✓
	Unavailable	✓	✓
Int. 2+	Revoked	✓	✓
	Unavailable	✗	✗
Leaf	Revoked	✓	✓
	Unavailable	✗	A
OCSP Stapling			
Request OCSP Staple		✓	✓
Respect Revoked Staple		✓	✓

Internet Explorer

Checks CRLs *and* OCSP

Often rejects if revocation info unavailable

- Pops up alert for leaf in IE 10+

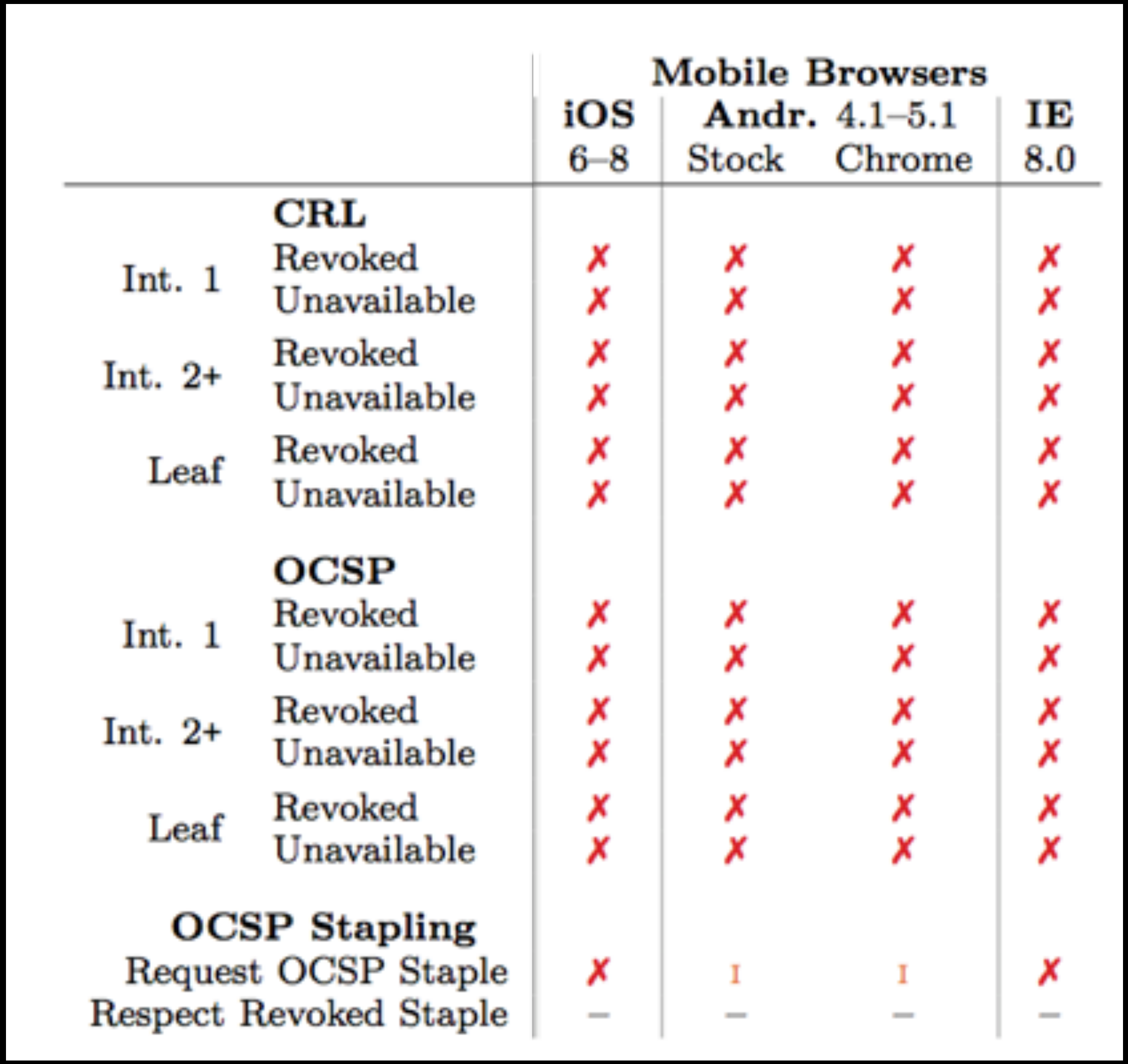
Supports OCSP stapling

✓ Passes test
✗ Fails test

EV Passes for EV certs
I Ignores OCSP Staple

A Pops up alert to user
L/W Passes on Linux/Win.

Results across all browsers



		Mobile Browsers			
		iOS	Andr. 4.1–5.1		IE
		6–8	Stock	Chrome	8.0
	CRL				
Int. 1	Revoked	✗	✗	✗	✗
	Unavailable	✗	✗	✗	✗
Int. 2+	Revoked	✗	✗	✗	✗
	Unavailable	✗	✗	✗	✗
Leaf	Revoked	✗	✗	✗	✗
	Unavailable	✗	✗	✗	✗
	OCSP				
Int. 1	Revoked	✗	✗	✗	✗
	Unavailable	✗	✗	✗	✗
Int. 2+	Revoked	✗	✗	✗	✗
	Unavailable	✗	✗	✗	✗
Leaf	Revoked	✗	✗	✗	✗
	Unavailable	✗	✗	✗	✗
OCSP Stapling					
Request OCSP Staple		✗	I	I	✗
Respect Revoked Staple		–	–	–	–

Mobile Browsers

Uniformly *never* check

Android browsers request Staple
…and promptly ignore it

✔ Passes test
✗ Fails test

EV Passes for EV certs
I Ignores OCSP Staple

A Pops up alert to user
L/W Passes on Linux/Win.