

An End-to-End Measurement of Certificate Revocation in the Web's PKI

Yabing Liu*, Will Tome*, Liang Zhang*, David Choffnes*, Dave Levin†, Bruce Maggs‡, Alan Mislove*, Aaron Schulman§, Christo Wilson*

*Northeastern University

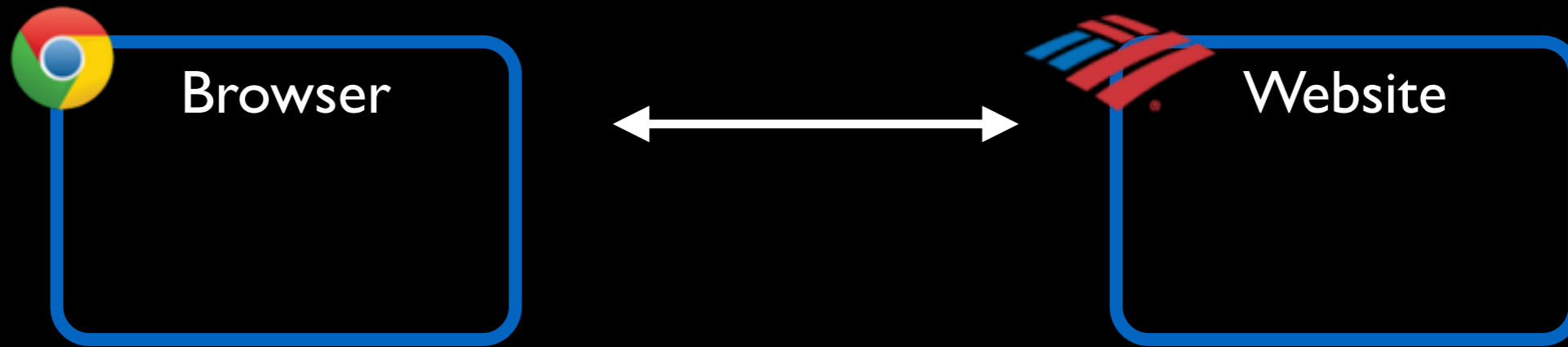
†University of Maryland

‡Duke University and Akamai Technologies

§Stanford University

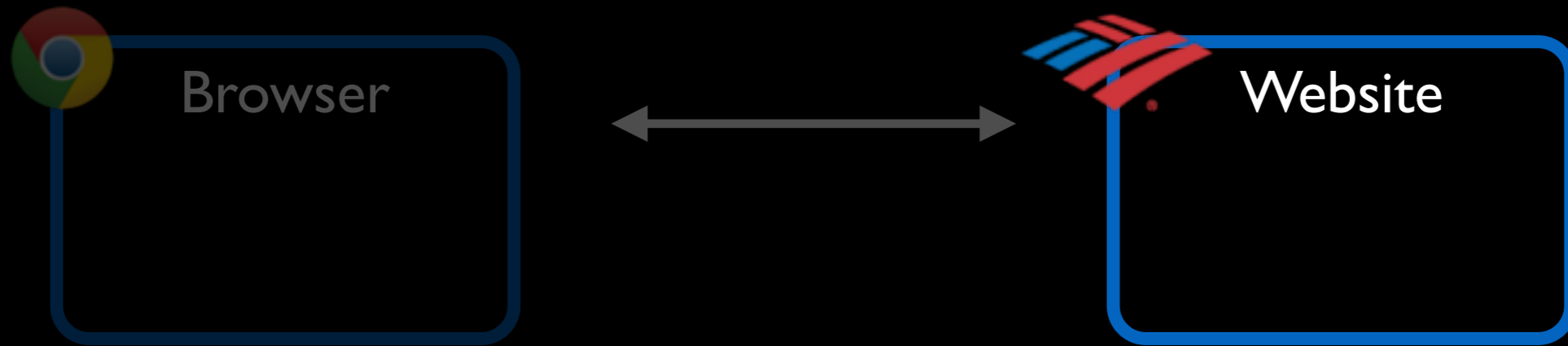
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



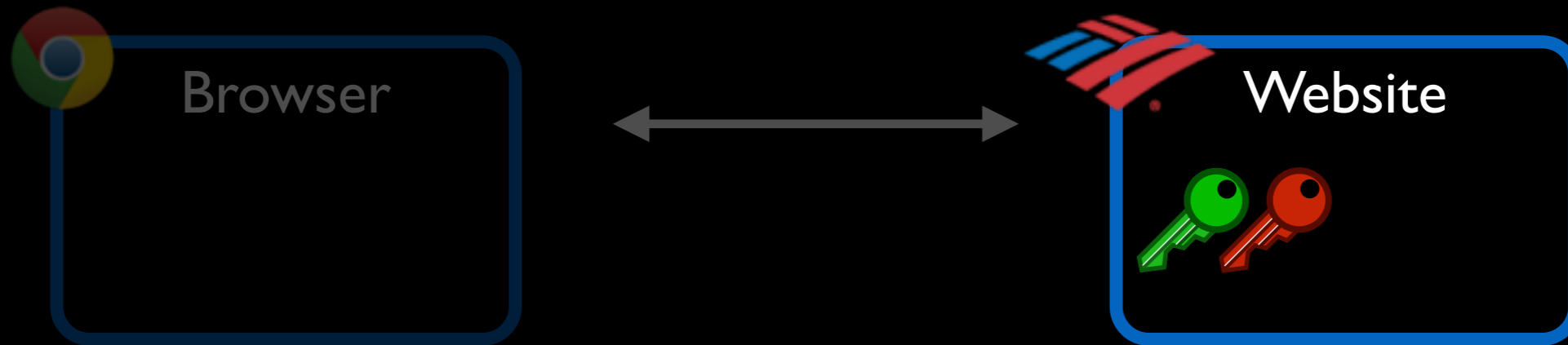
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



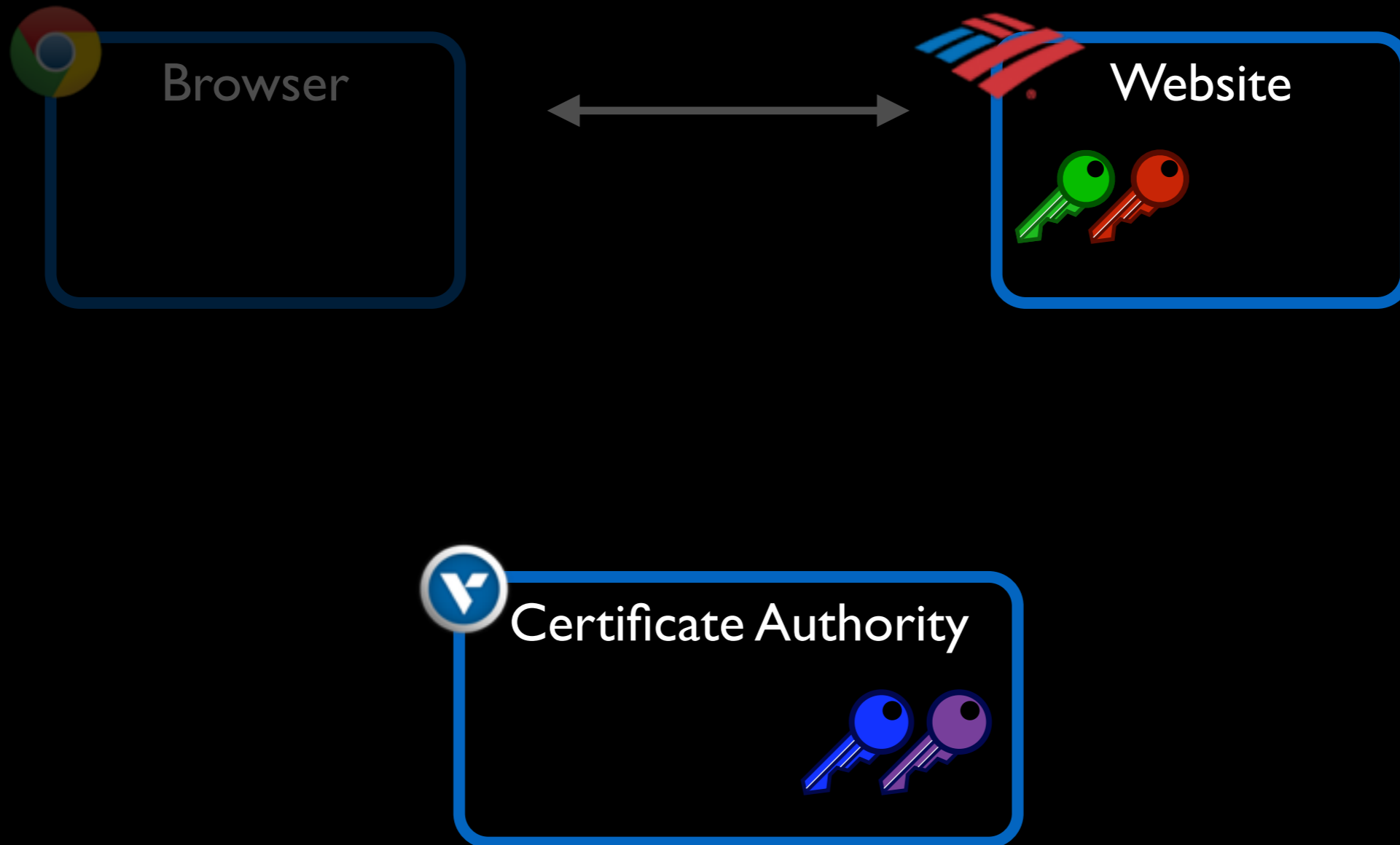
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



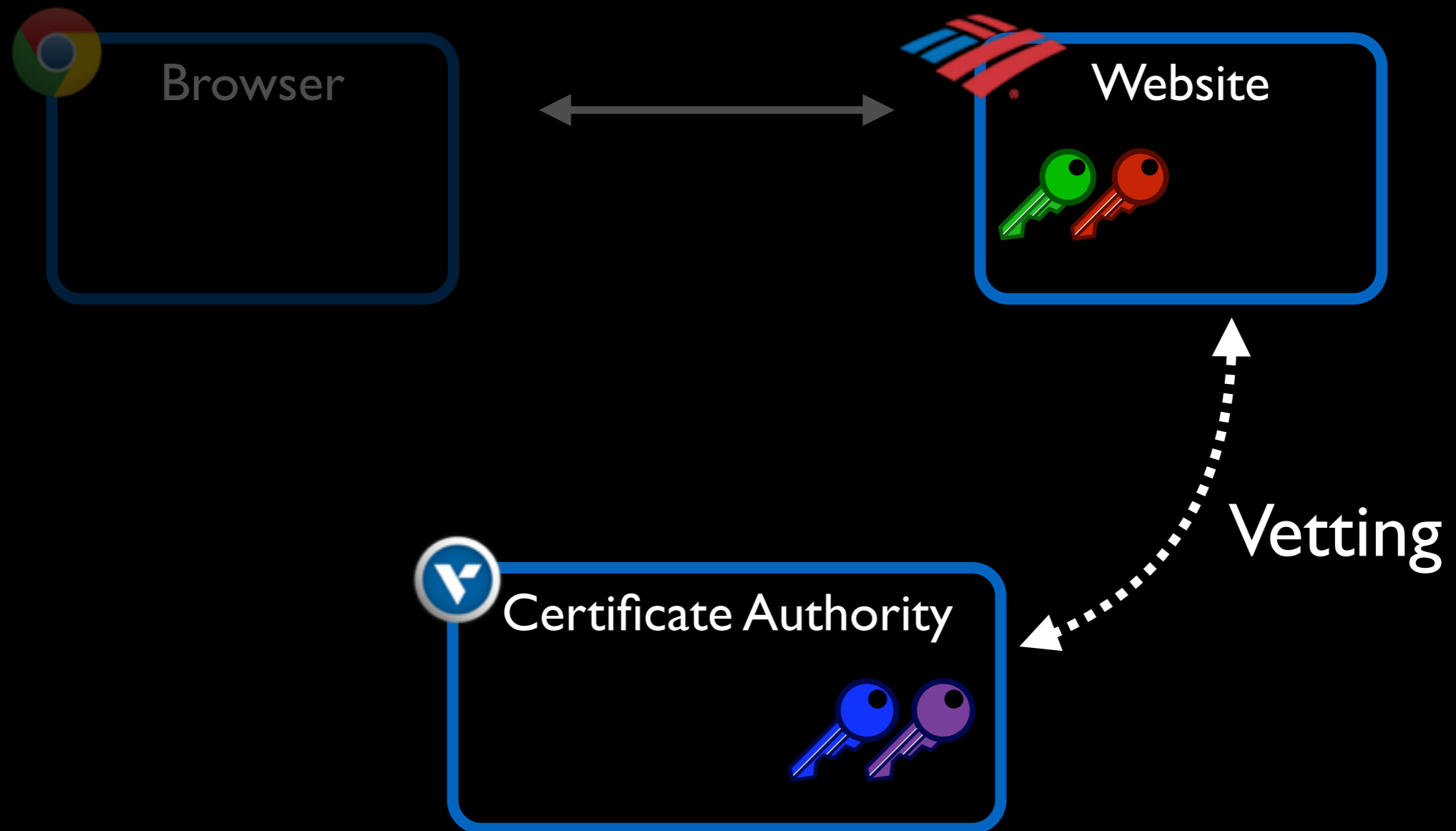
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



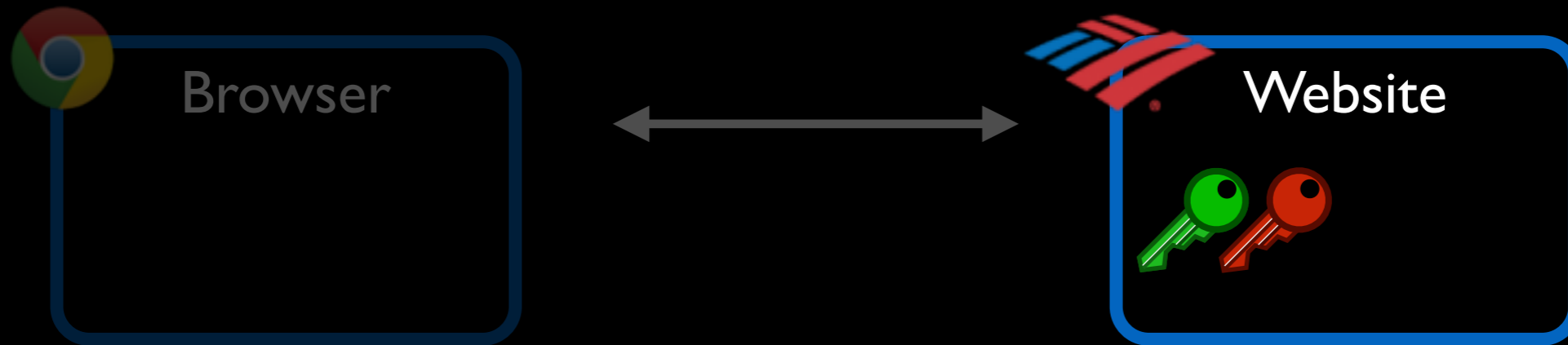
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



Public Key Infrastructures (PKIs)

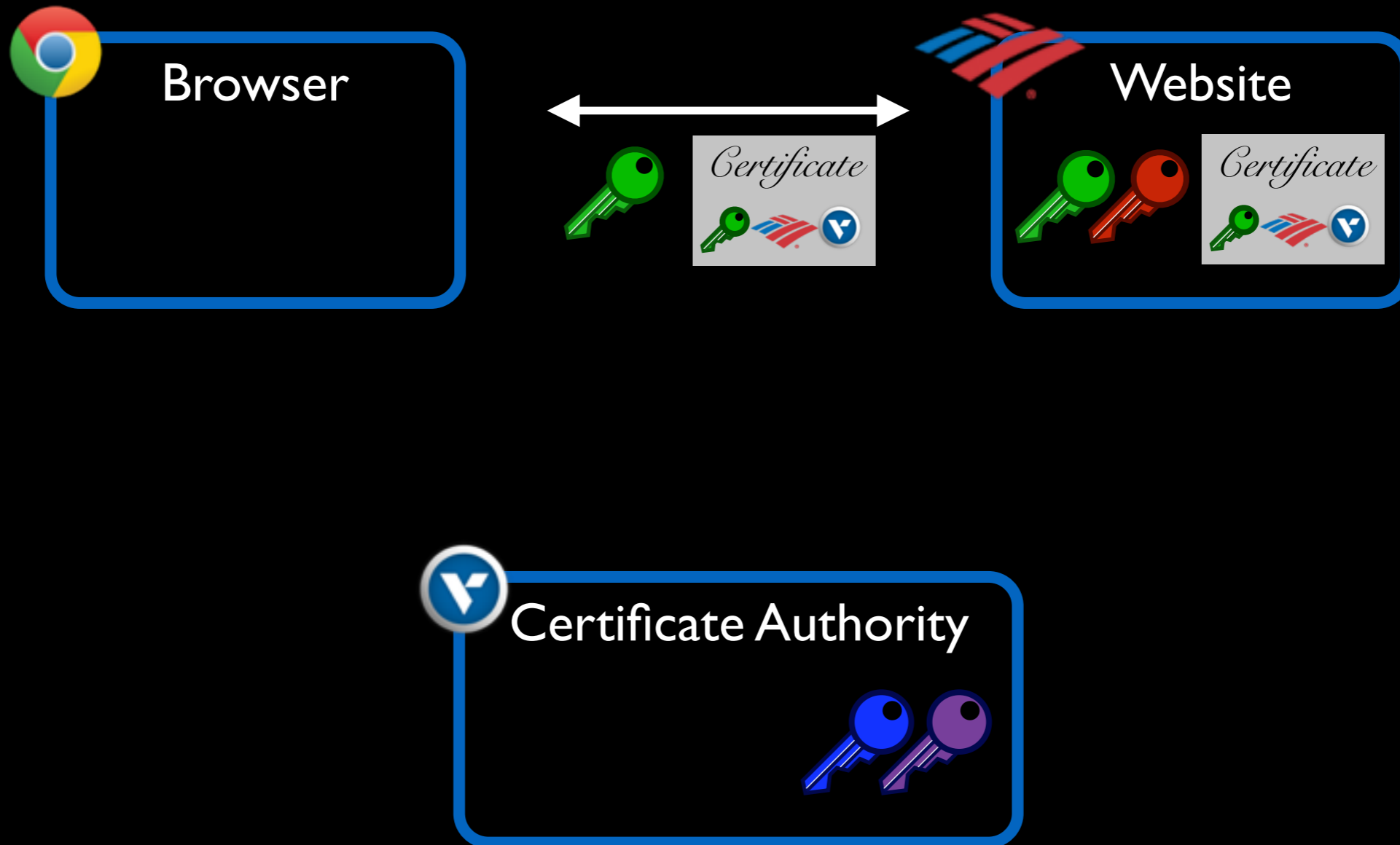
How can users truly know with whom they are communicating?



Certificate

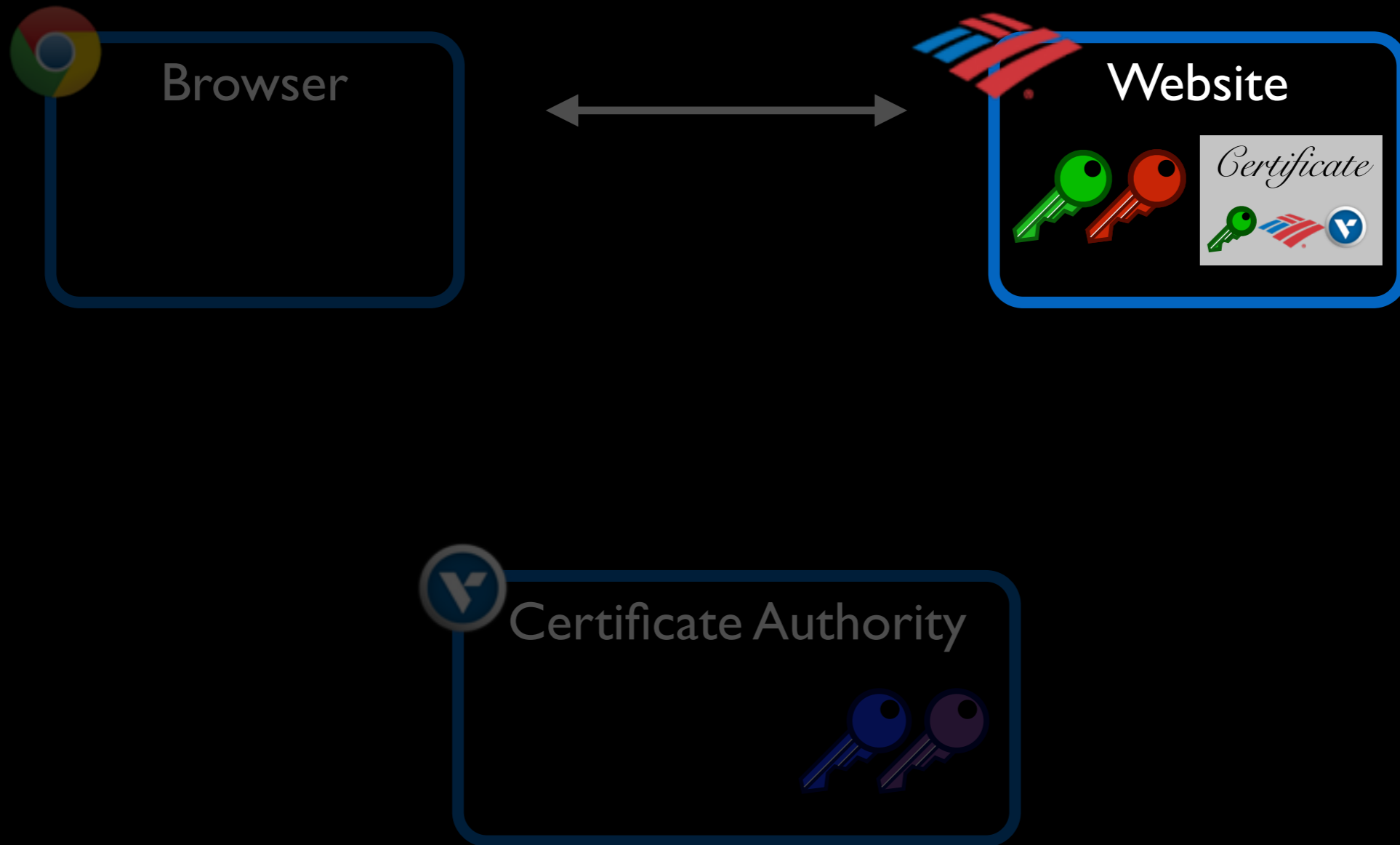
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



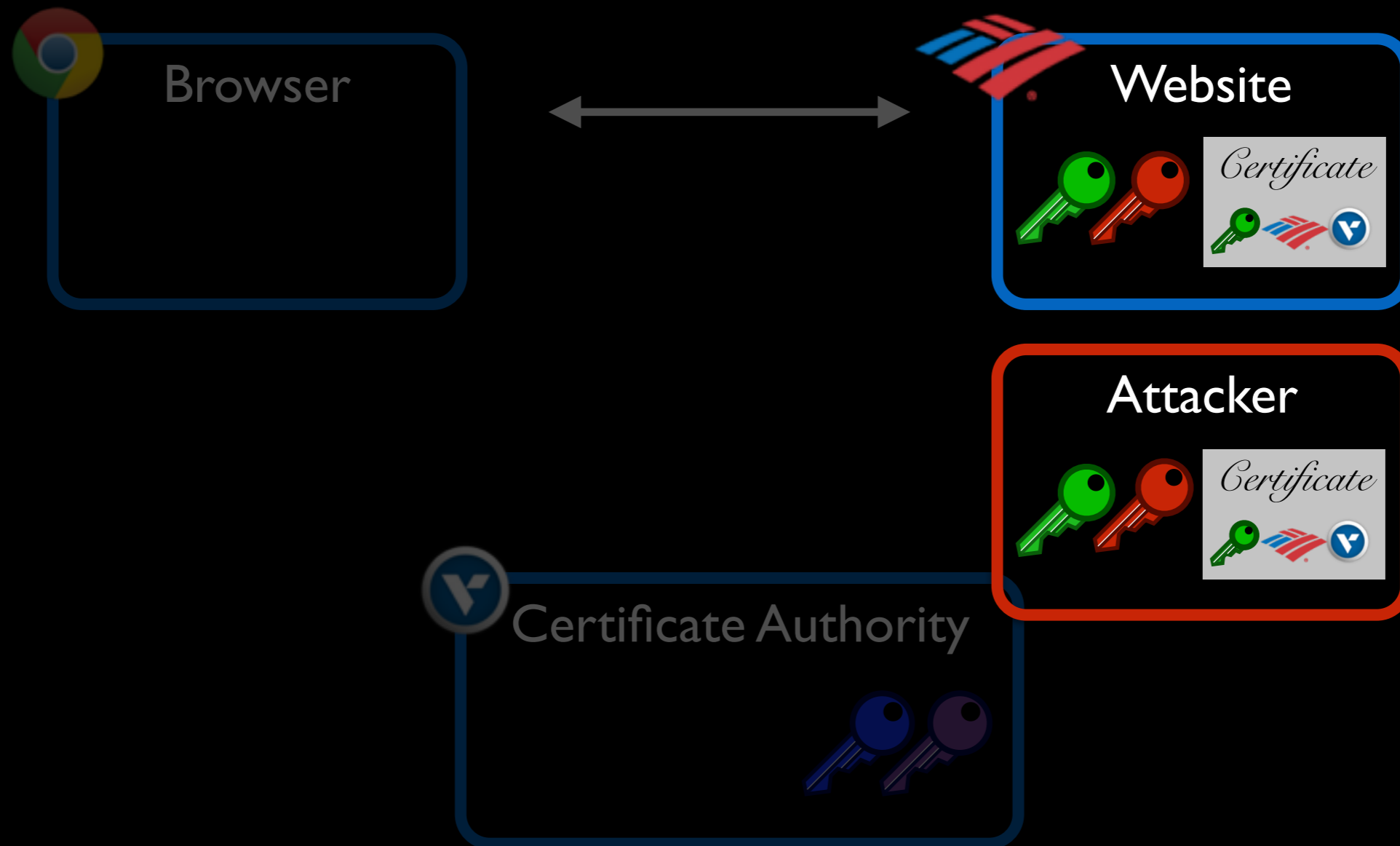
Certificate revocation

What happens when a certificate is no longer valid?



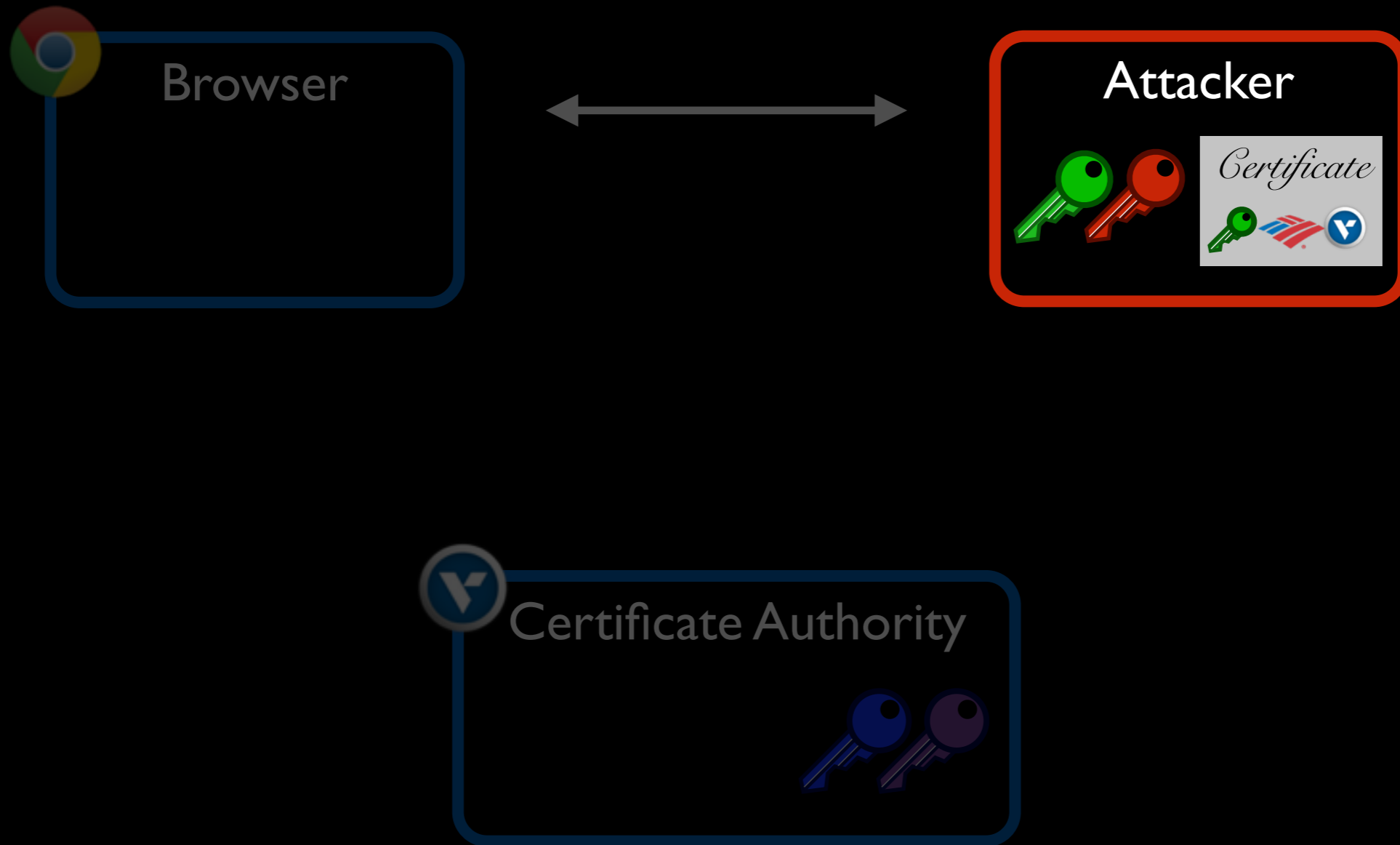
Certificate revocation

What happens when a certificate is no longer valid?



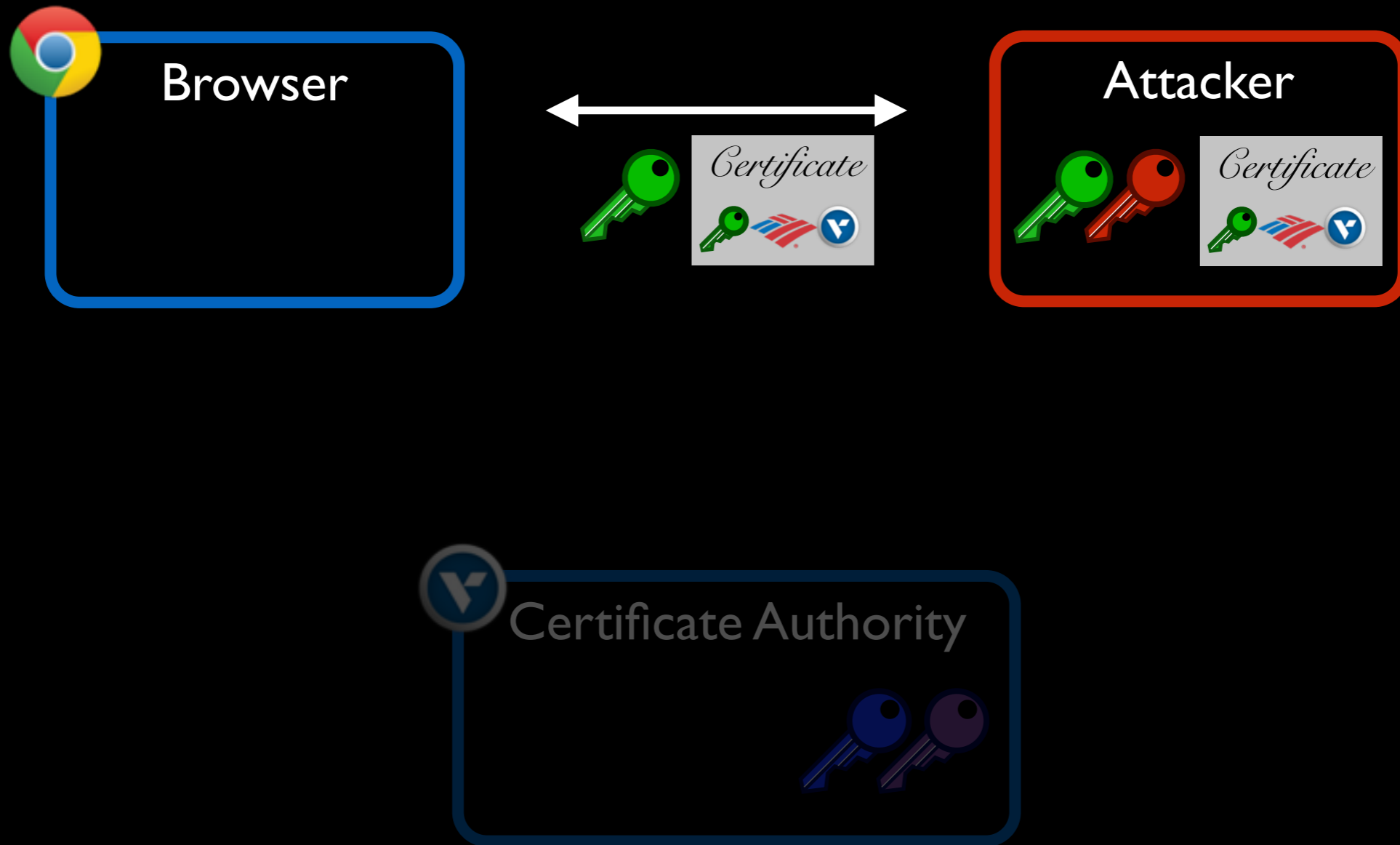
Certificate revocation

What happens when a certificate is no longer valid?



Certificate revocation

What happens when a certificate is no longer valid?



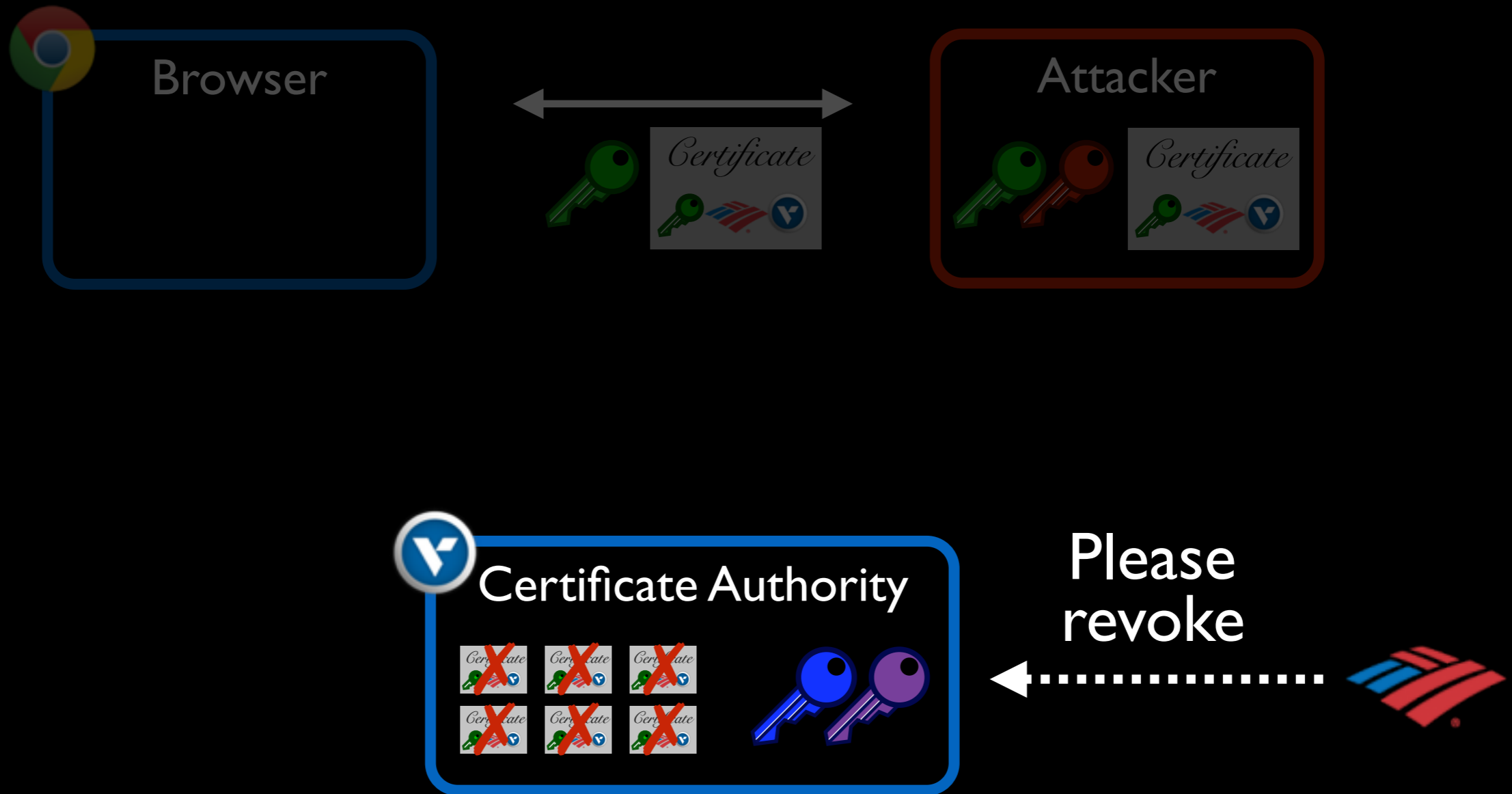
Certificate revocation

What happens when a certificate is no longer valid?



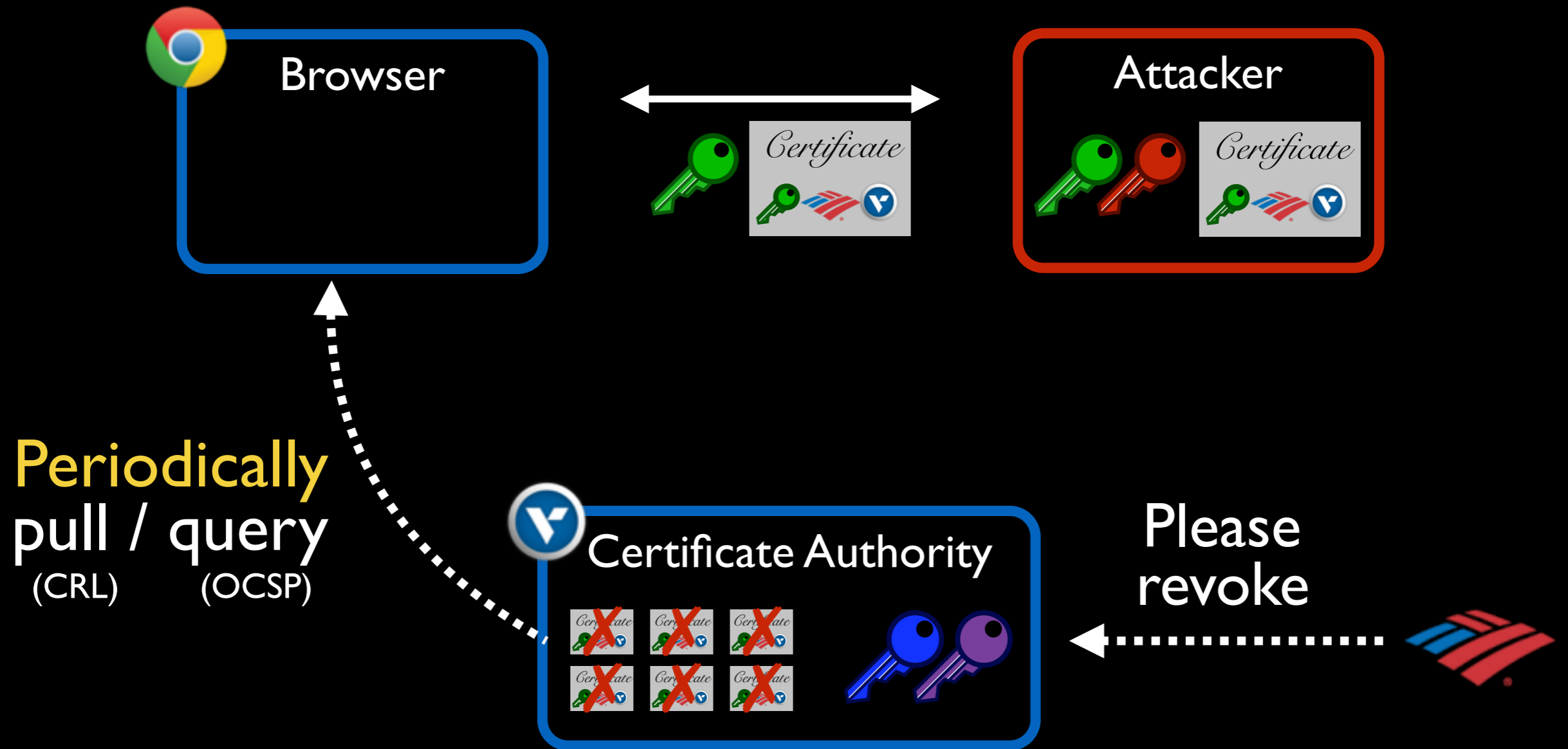
Certificate revocation

What happens when a certificate is no longer valid?



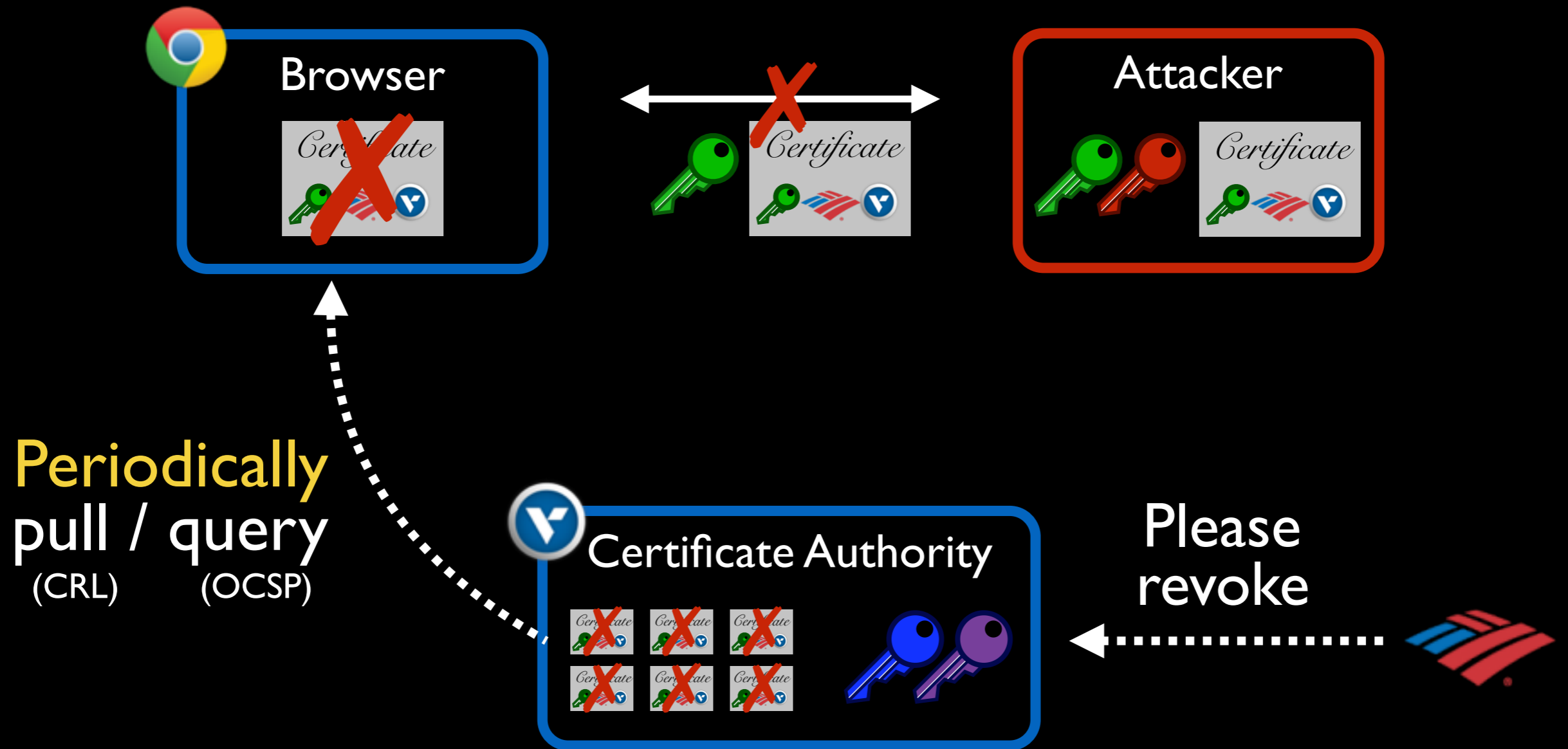
Certificate revocation

What happens when a certificate is no longer valid?



Certificate revocation

What happens when a certificate is no longer valid?



Certificate revocation responsibilities



Administrators must **revoke certificates** when keys are compromised



Certificate authorities must **publish revocations** as quickly as possible



Browsers must **check revocation status** on each connection

This talk:

Do these entities do what they need to do?

Outline



Website admin behavior

e.g., **what is the frequency of revocation?**



Certificate authorities behavior

e.g., **how do CAs serve revocations?**



Client behavior

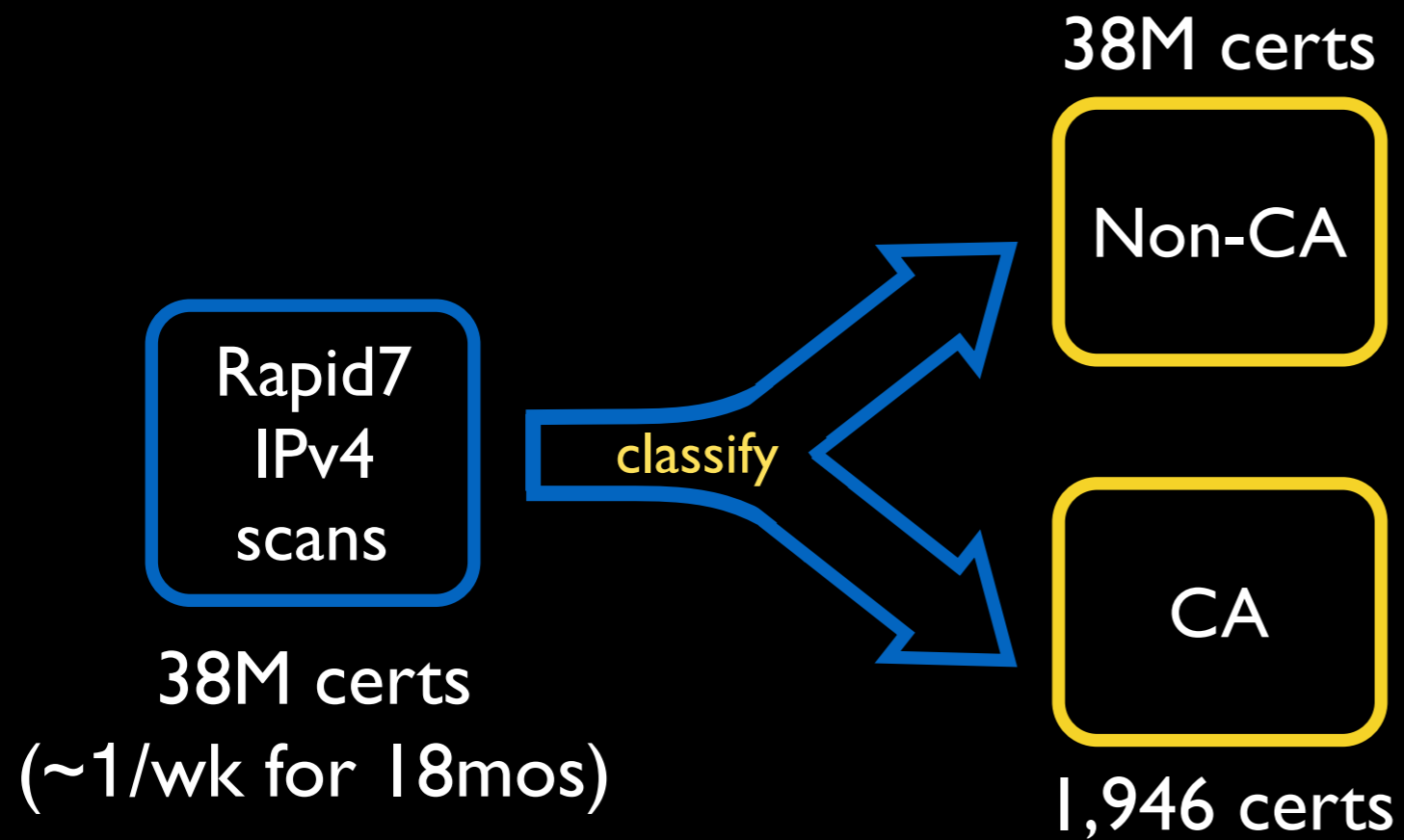
e.g., **do browsers check revocations?**

Dataset

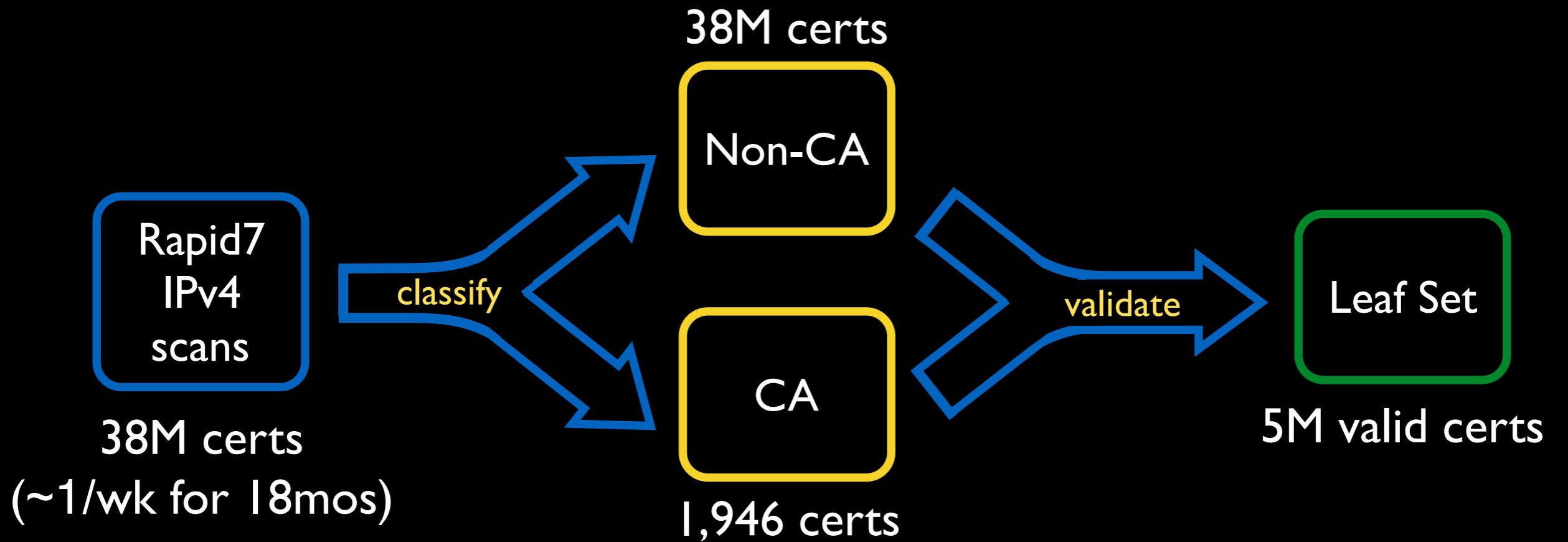
Rapid7
IPv4
scans

38M certs
(~1/wk for 18mos)

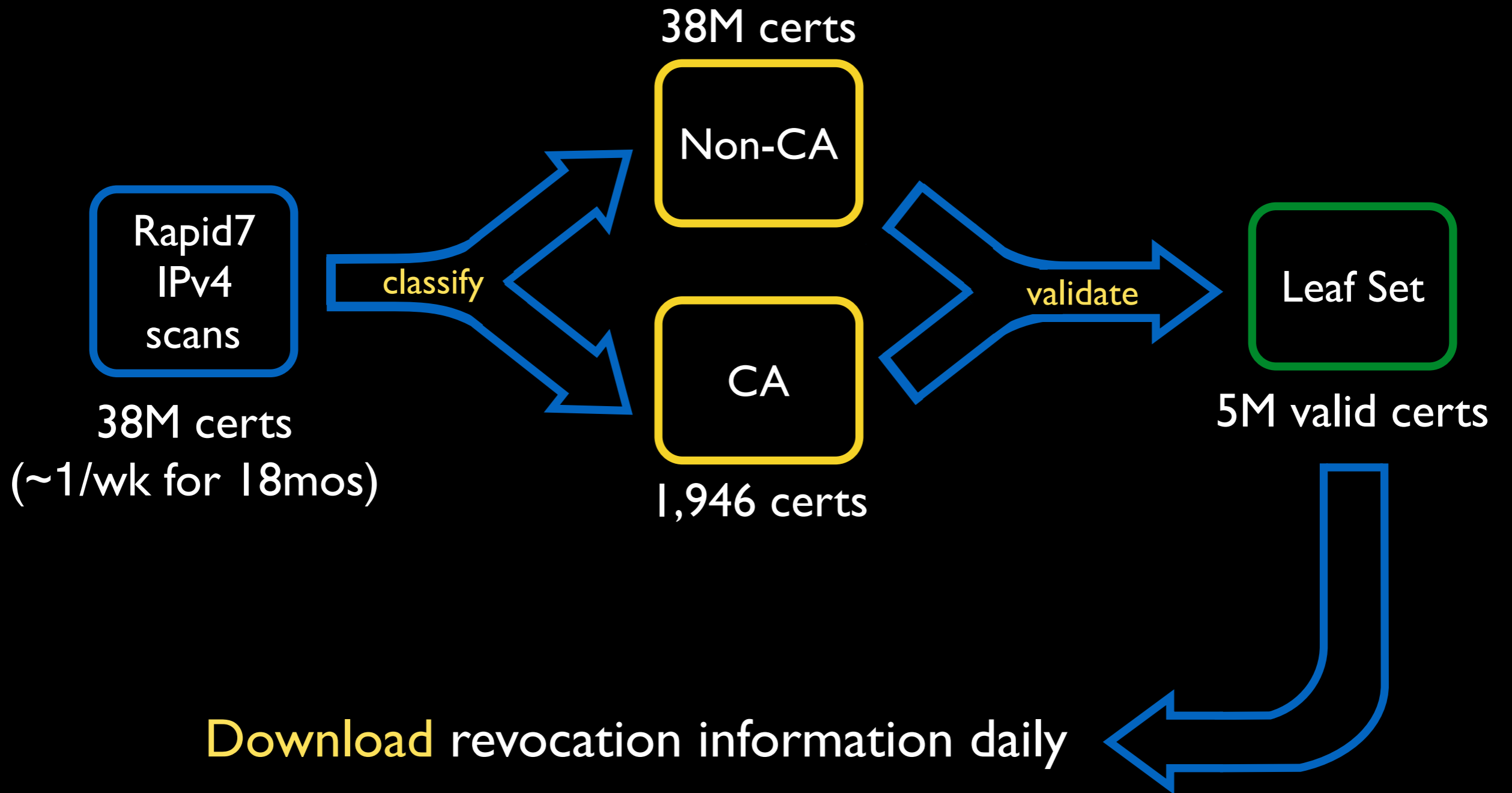
Dataset



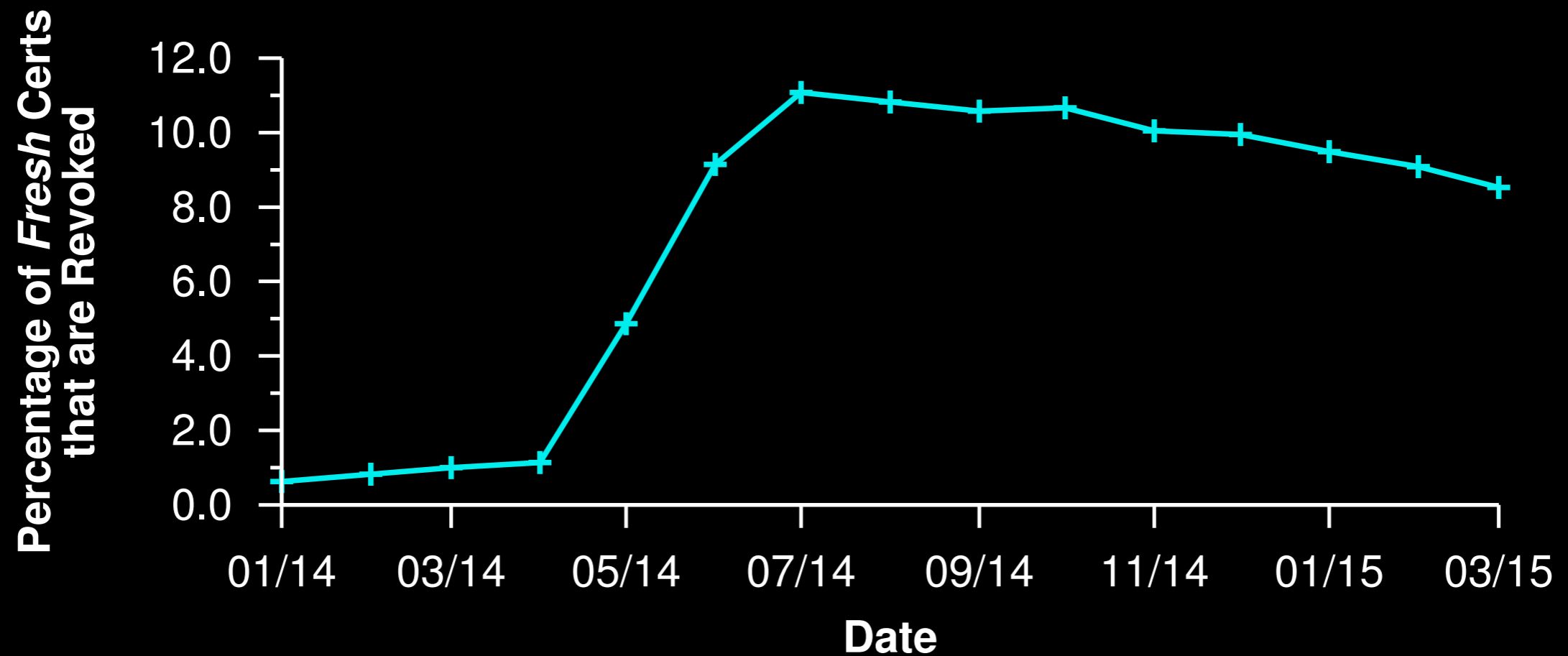
Dataset



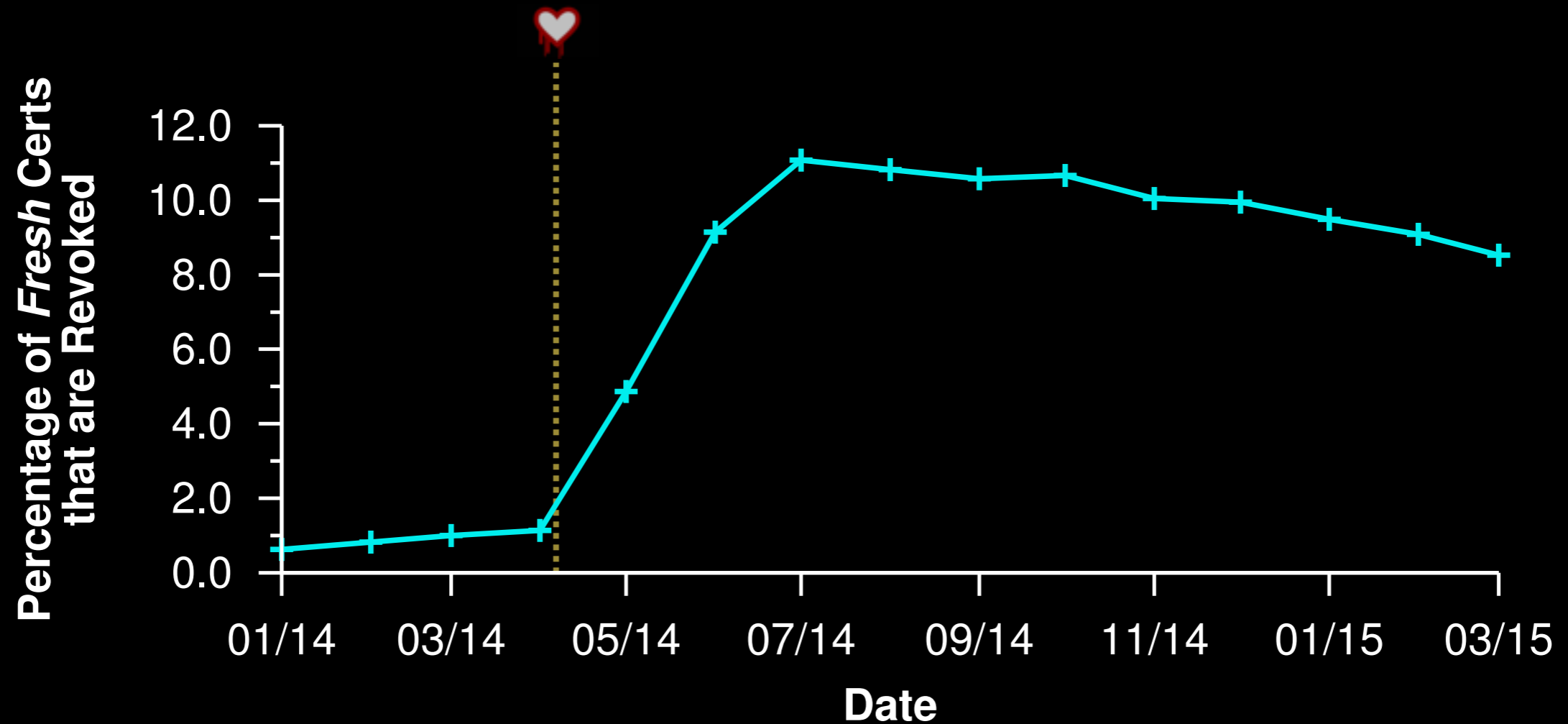
Dataset



How frequently are certificates revoked?

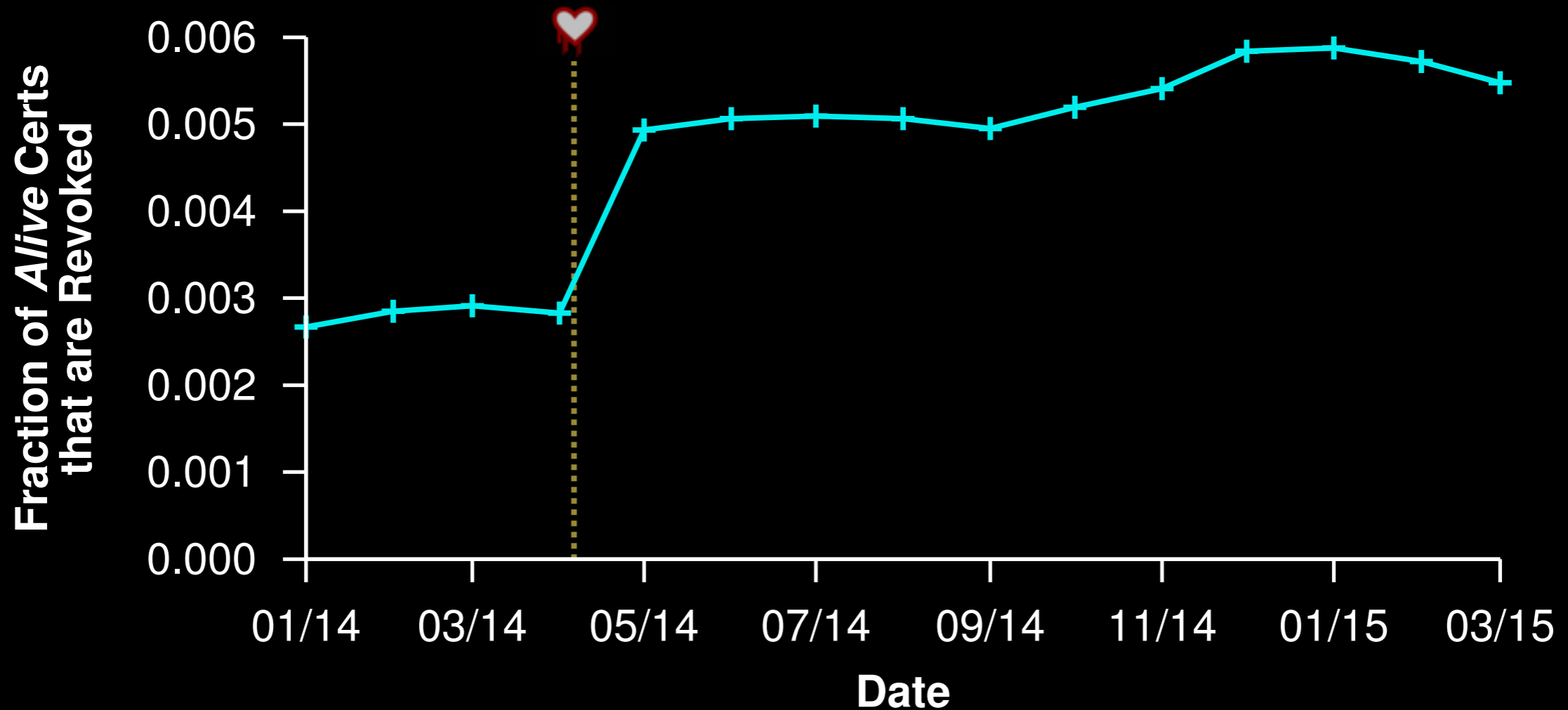


How frequently are certificates revoked?



Significant fraction of certificates revoked
1% in steady state; more than 8% after Heartbleed

Are there revoked certificates being used?



Over 0.5% advertised certificates are revoked
Website admins failed to update their servers

Outline



Website admin behavior
e.g., **revocation is common ~8%**

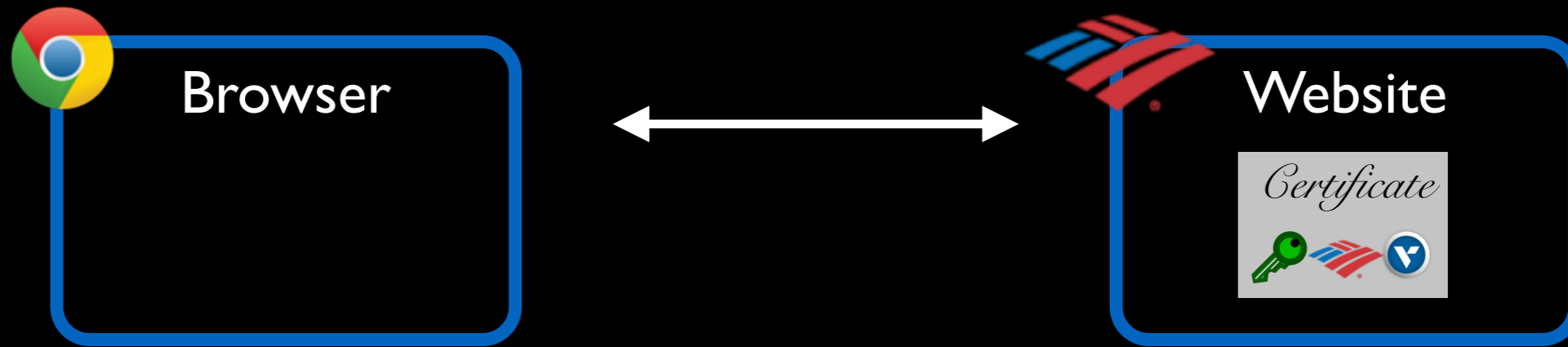


Certificate authorities behavior
e.g., **how do CAs serve revocations?**

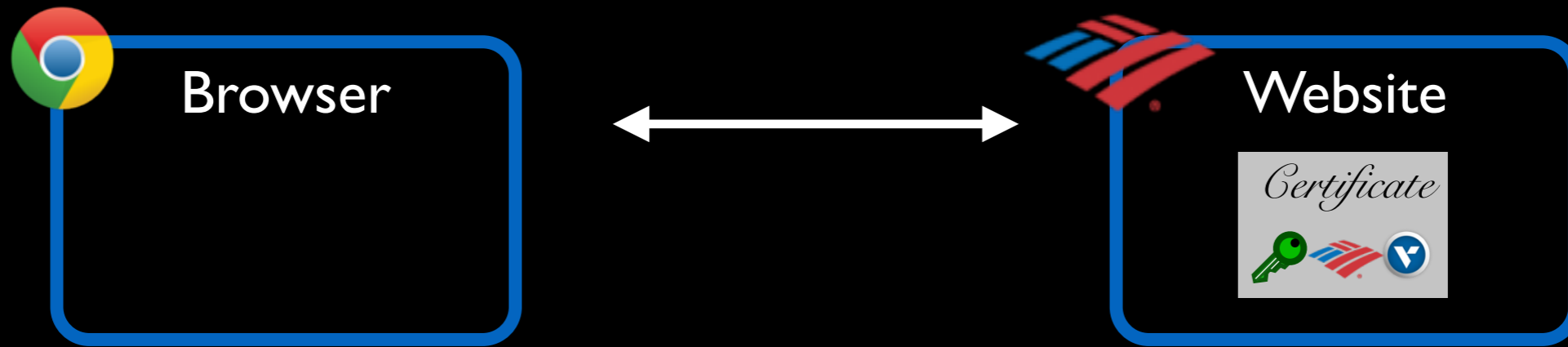


Client behavior
e.g., **do browsers check revocations?**

CRLs, OCSP, and OCSP Stapling



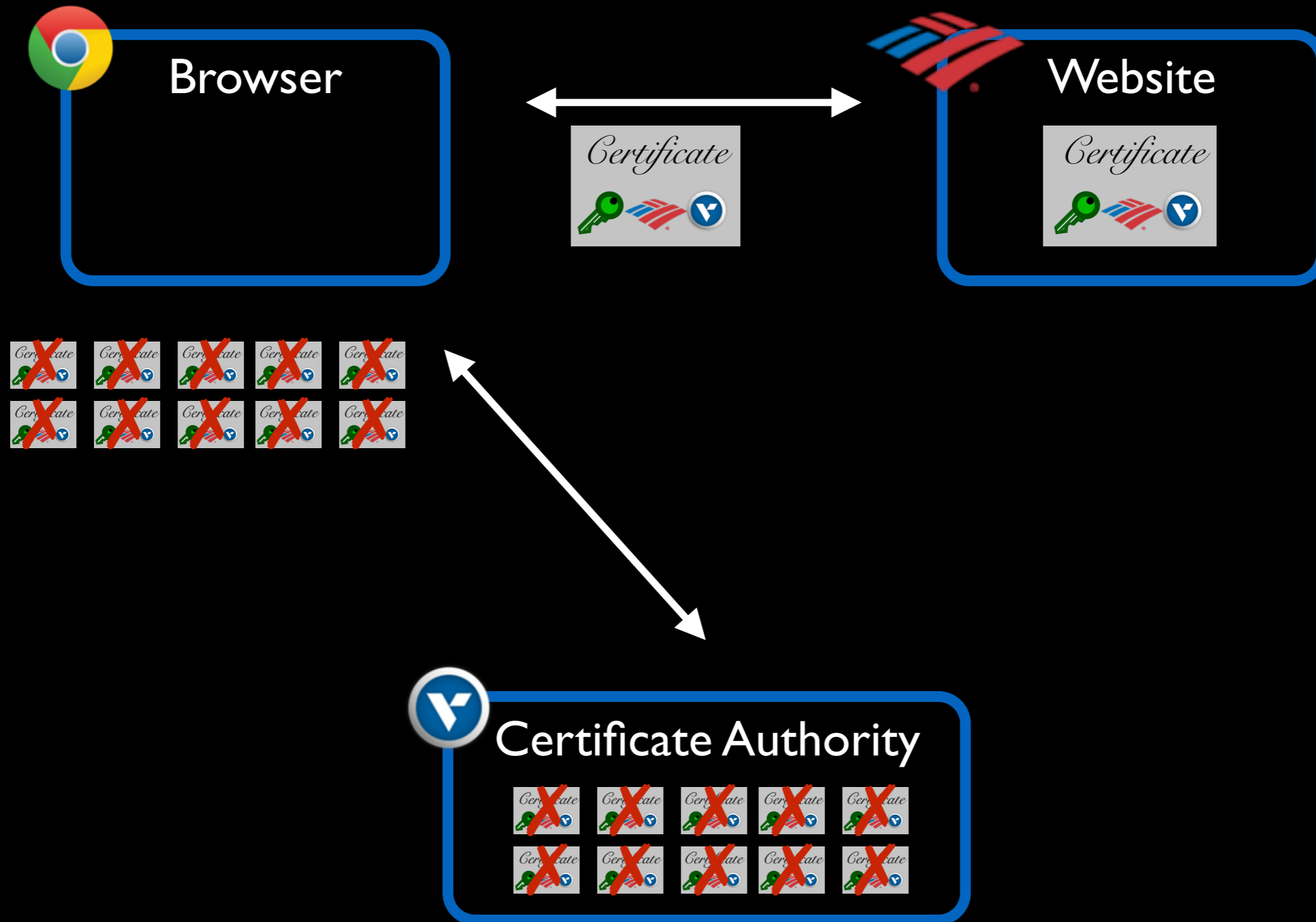
CRLs, OCSP, and OCSP Stapling



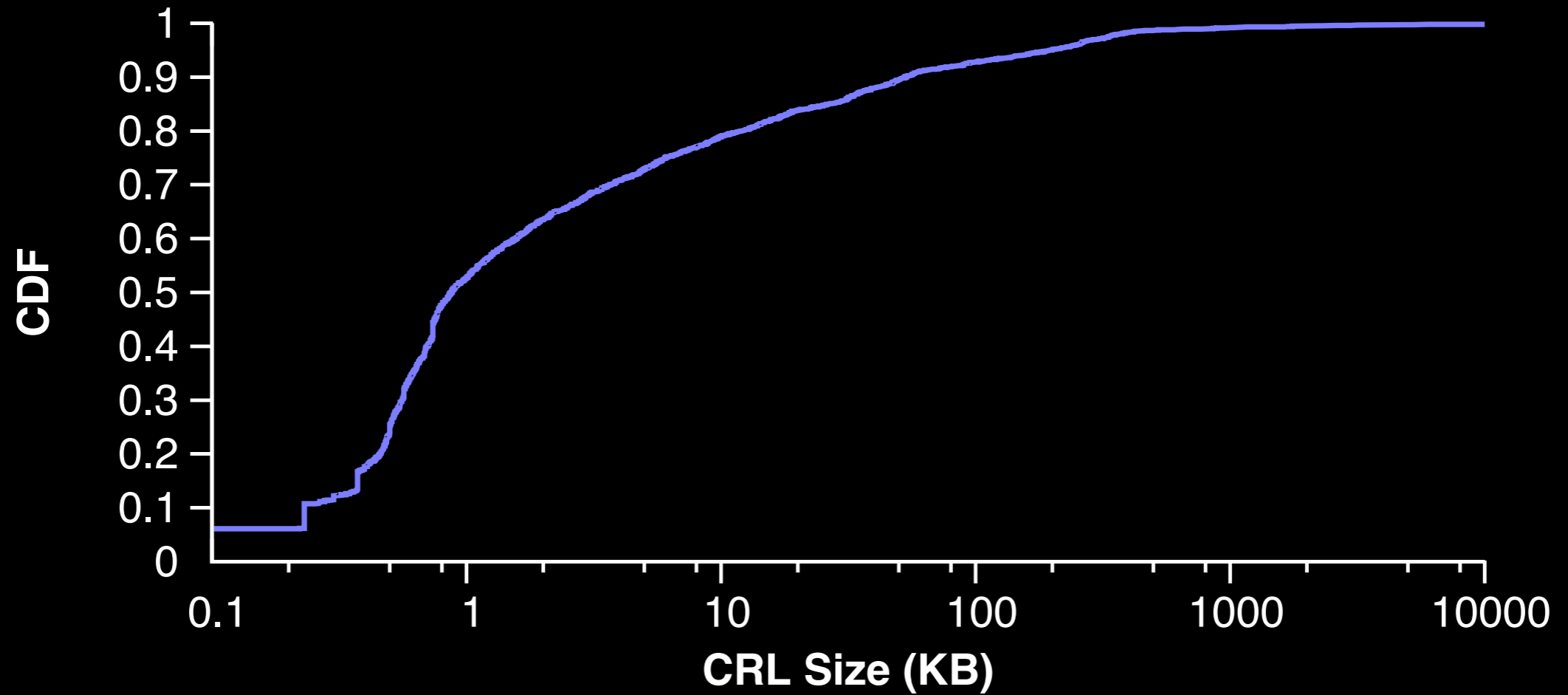
CRLs, OCSP, and OCSP Stapling



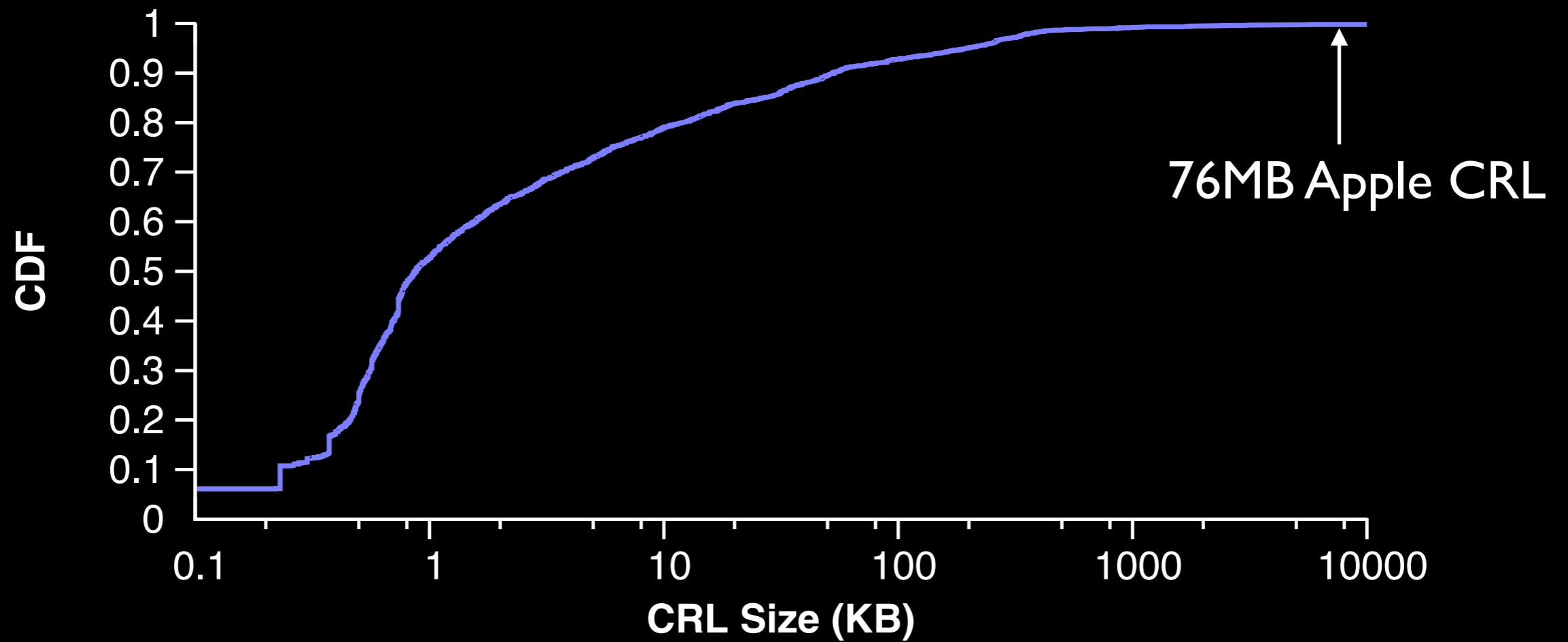
CRLs, OCSP, and OCSP Stapling



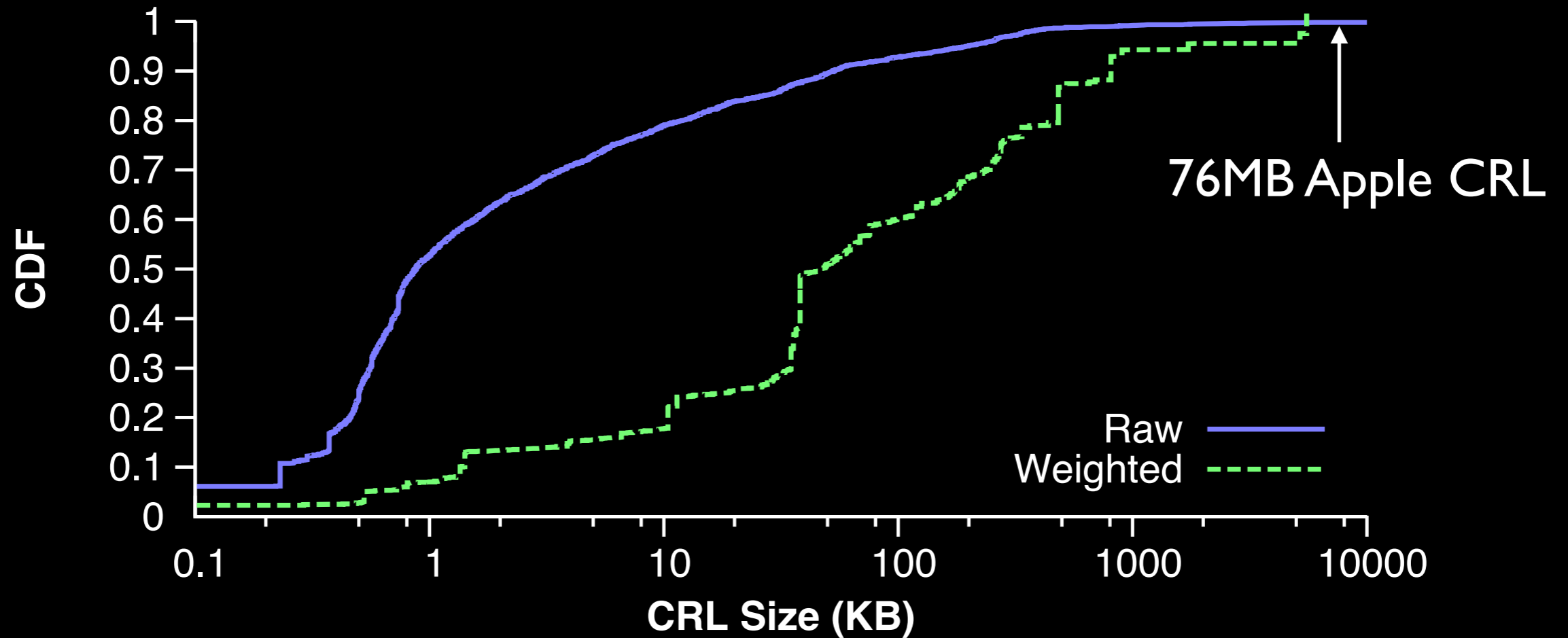
Cost of obtaining CRLs



Cost of obtaining CRLs



Cost of obtaining CRLs



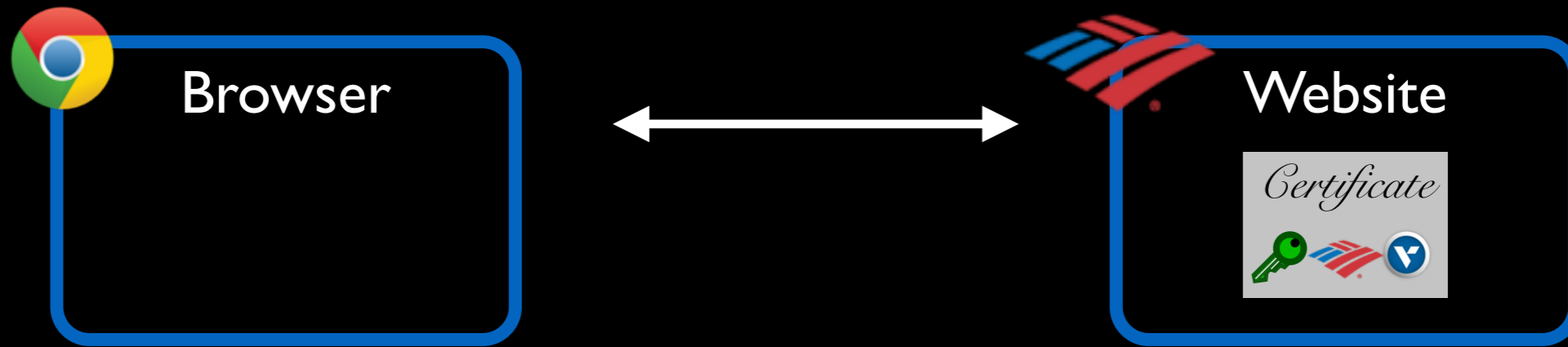
Most CRLs small, but large CRLs downloaded more often
Result: 50% of certs have CRLs larger than 45KB

CRLs from different CAs

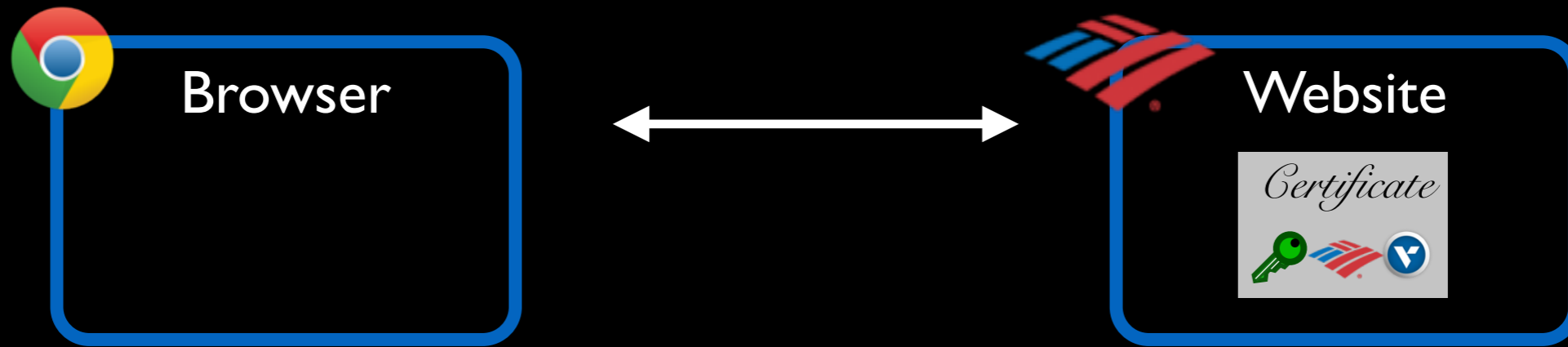
CA	Unique CRLs	Certificates		Avg. CRL size (KB)
		Total	Revoked	
GoDaddy	322	1,050,014	277,500	1,184.0
RapidSSL	5	626,774	2,153	34.5
Comodo	30	447,506	7,169	517.6
PositiveSSL	3	415,075	8,177	441.3
Verisign	37	311,788	15,438	205.2

CAs use only a small number of CRLs

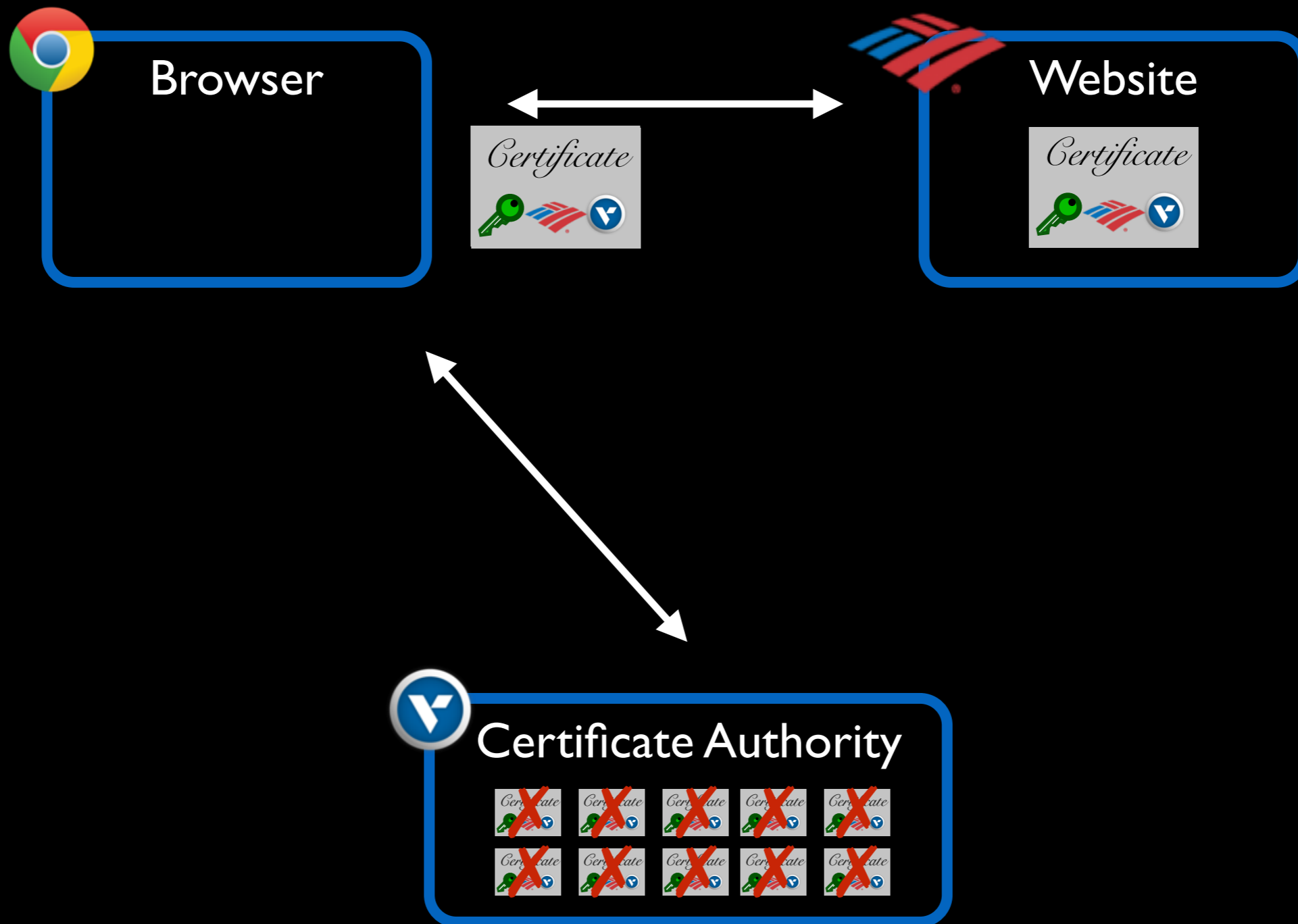
CRLs, OCSP, and OCSP Stapling



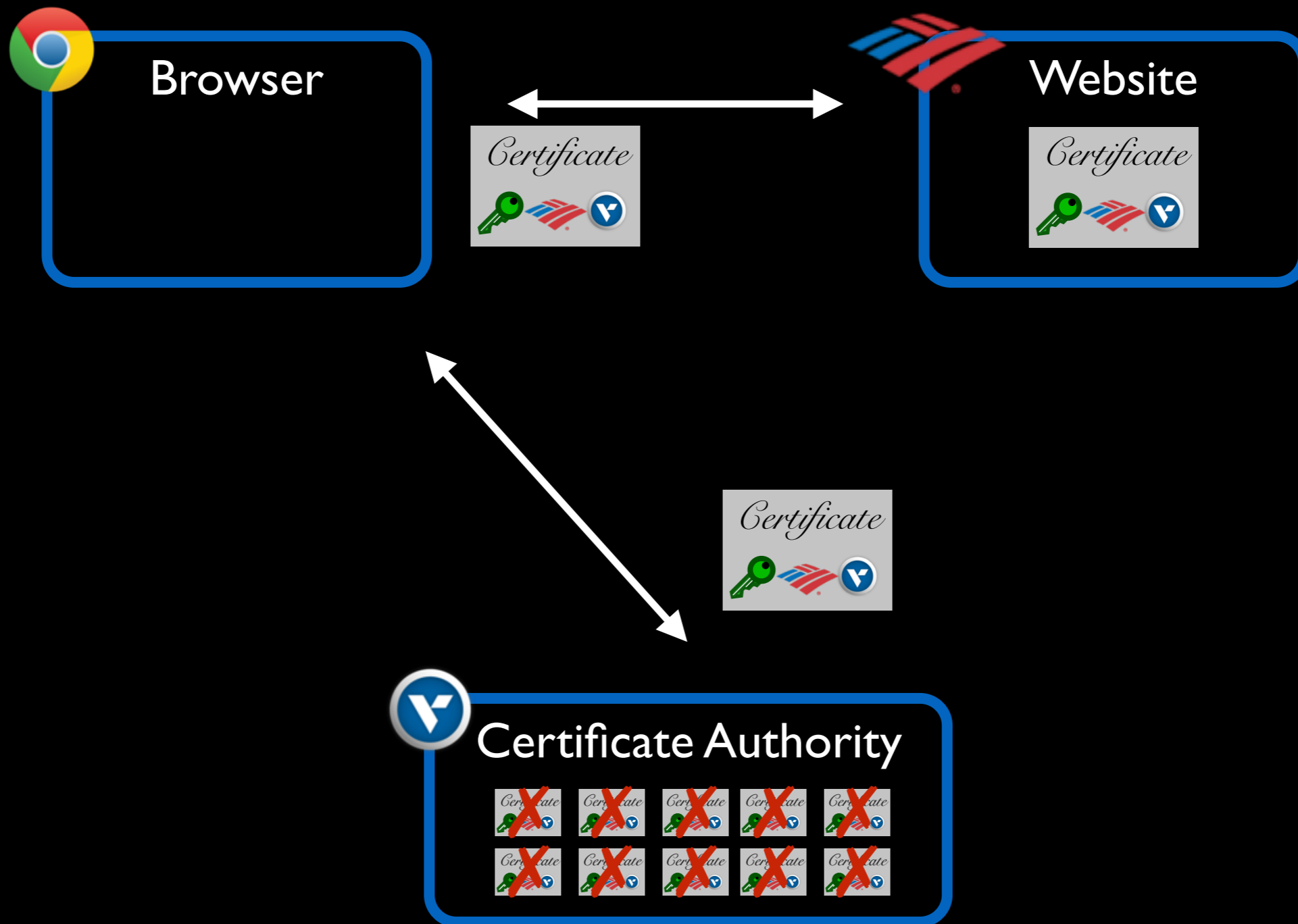
CRLs, OCSP, and OCSP Stapling



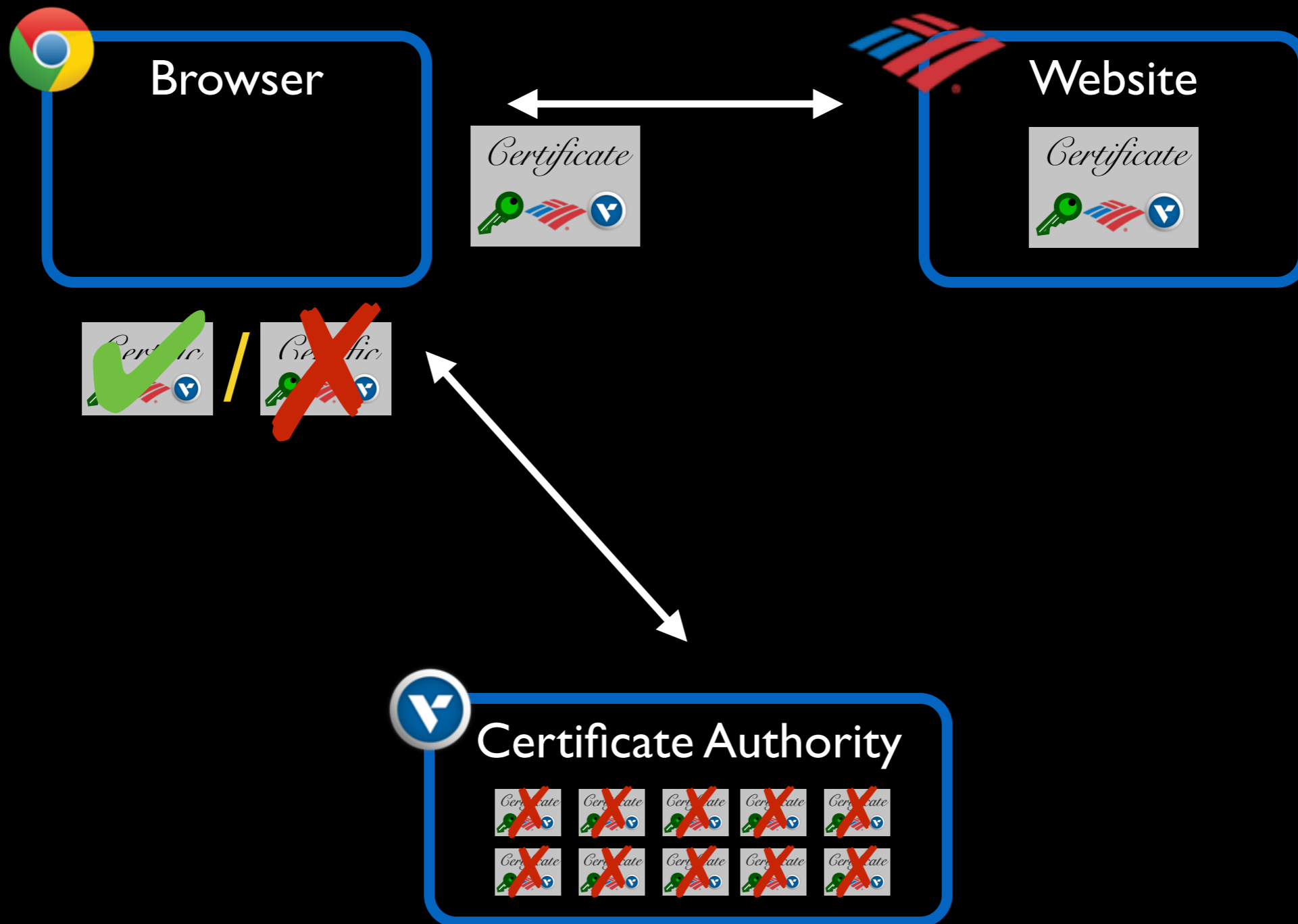
CRLs, OCSP, and OCSP Stapling



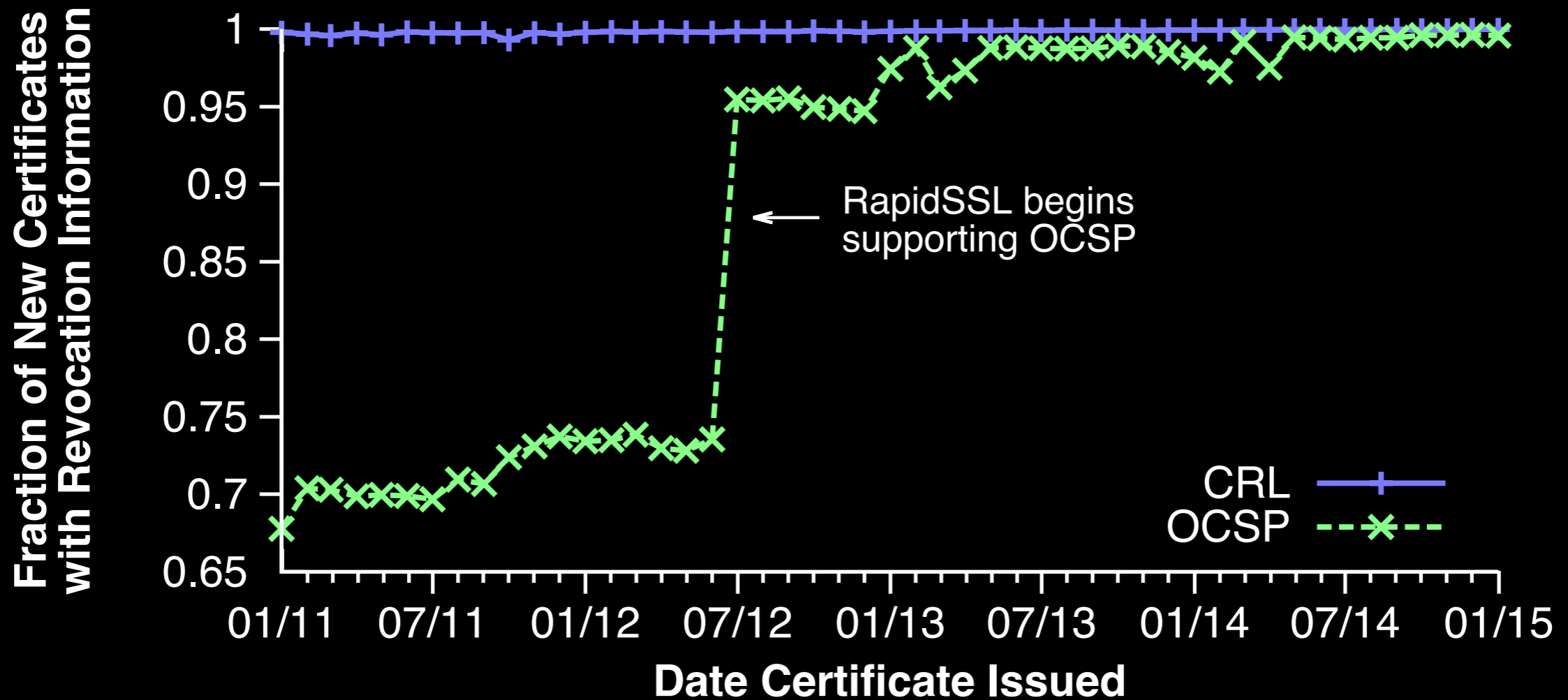
CRLs, OCSP, and OCSP Stapling



CRLs, OCSP, and OCSP Stapling

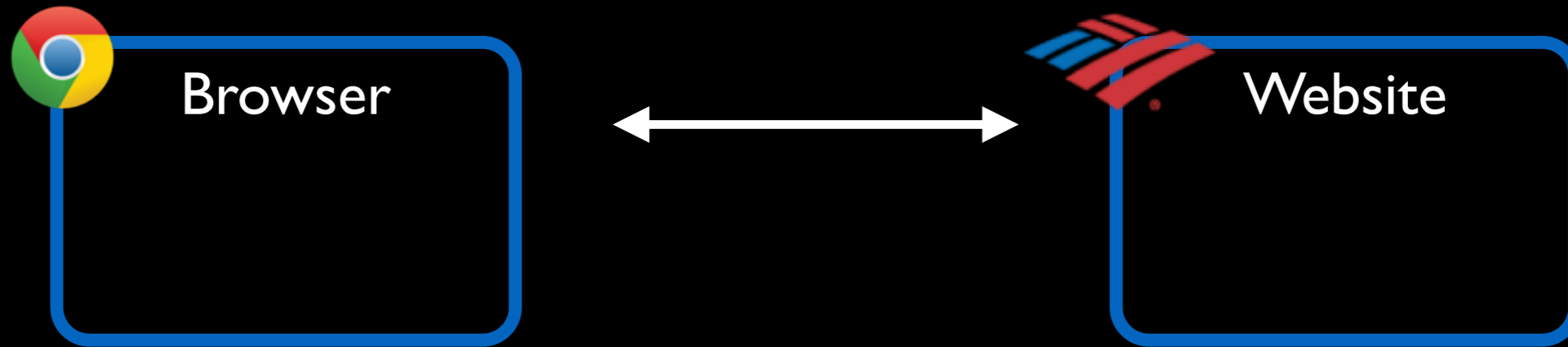


OCSP prevalence

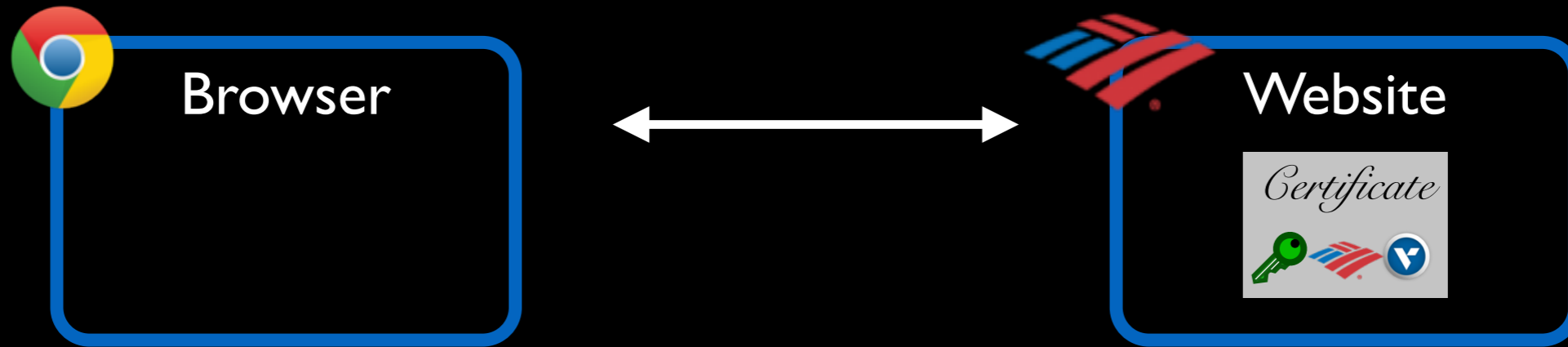


OCSP now universally supported

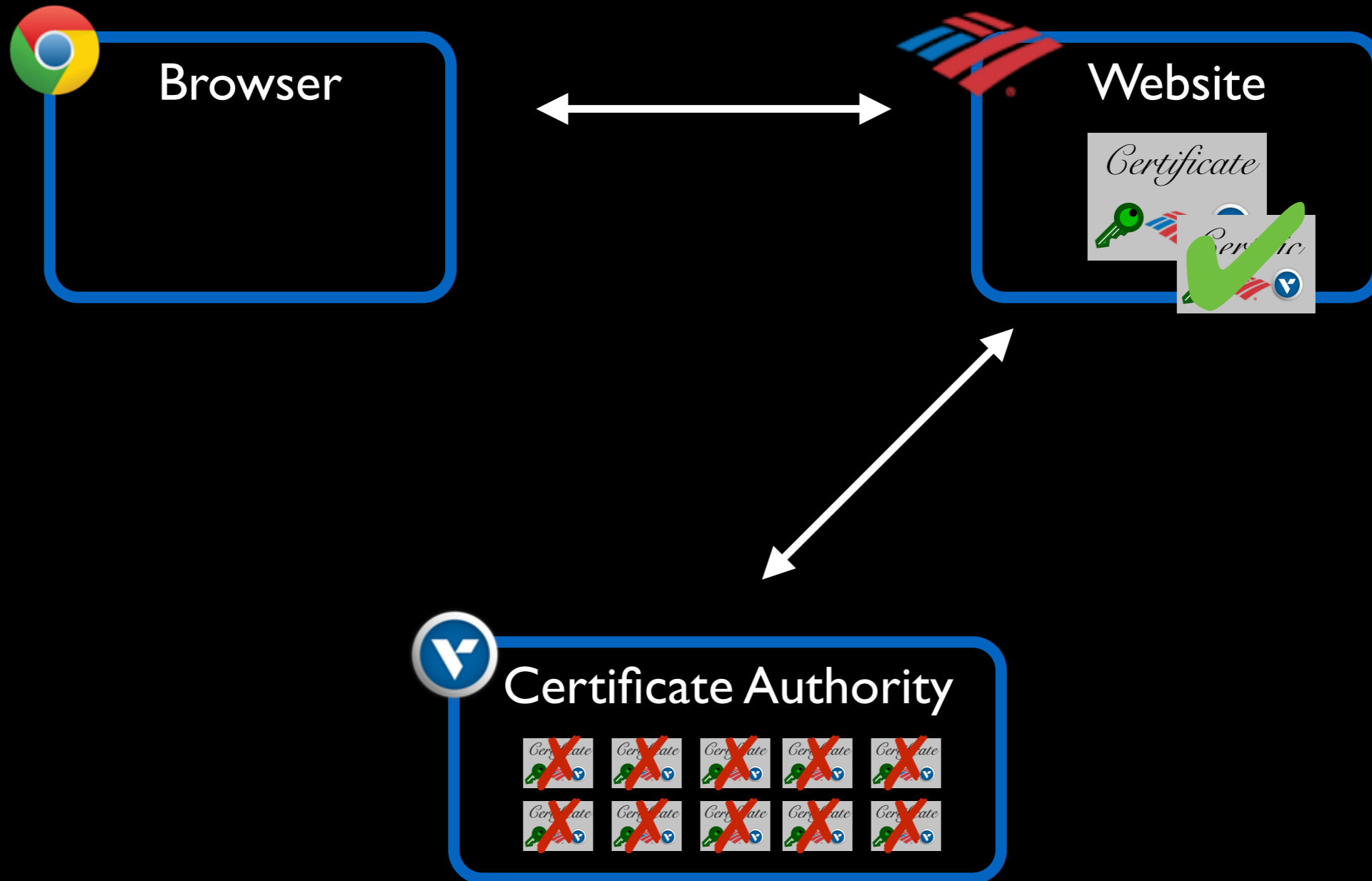
CRLs, OCSP, and OCSP Stapling



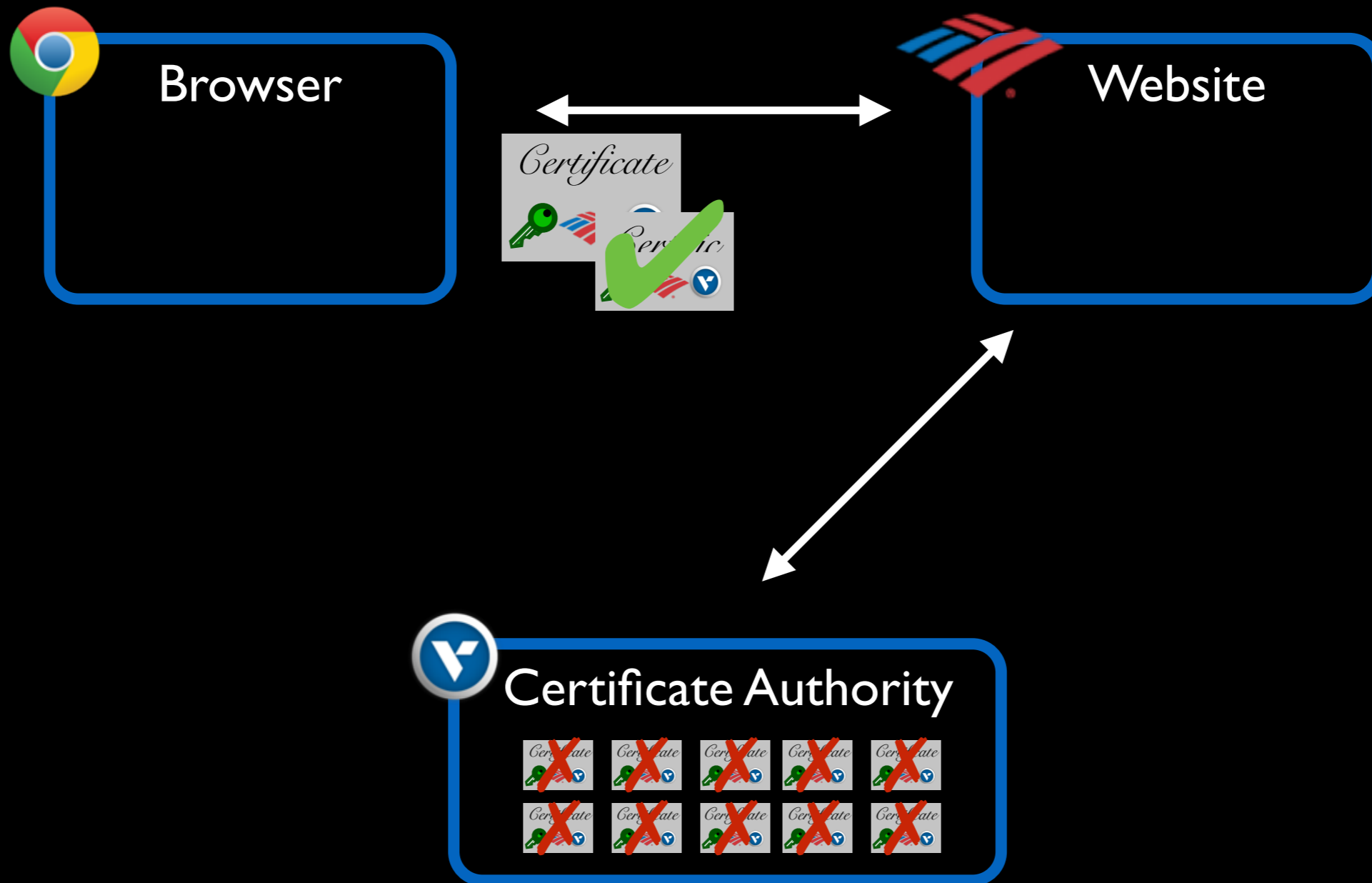
CRLs, OCSP, and OCSP Stapling



CRLs, OCSP, and OCSP Stapling



CRLs, OCSP, and OCSP Stapling



Limited OCSP Stapling Support

- IPv4 TLS Handshake scans by University of Michigan on 3/28/15
 - Every IPv4 server on port 443
 - Look for OCSP stapling support
- 2.2M valid certificates
 - 5.19% served by at least one server supports OCSP Stapling
 - 3.09% served by servers that all support OCSP Stapling

Website admins rarely enable OCSP Stapling

Outline



Website admin behavior
e.g., **revocation is common ~8%**

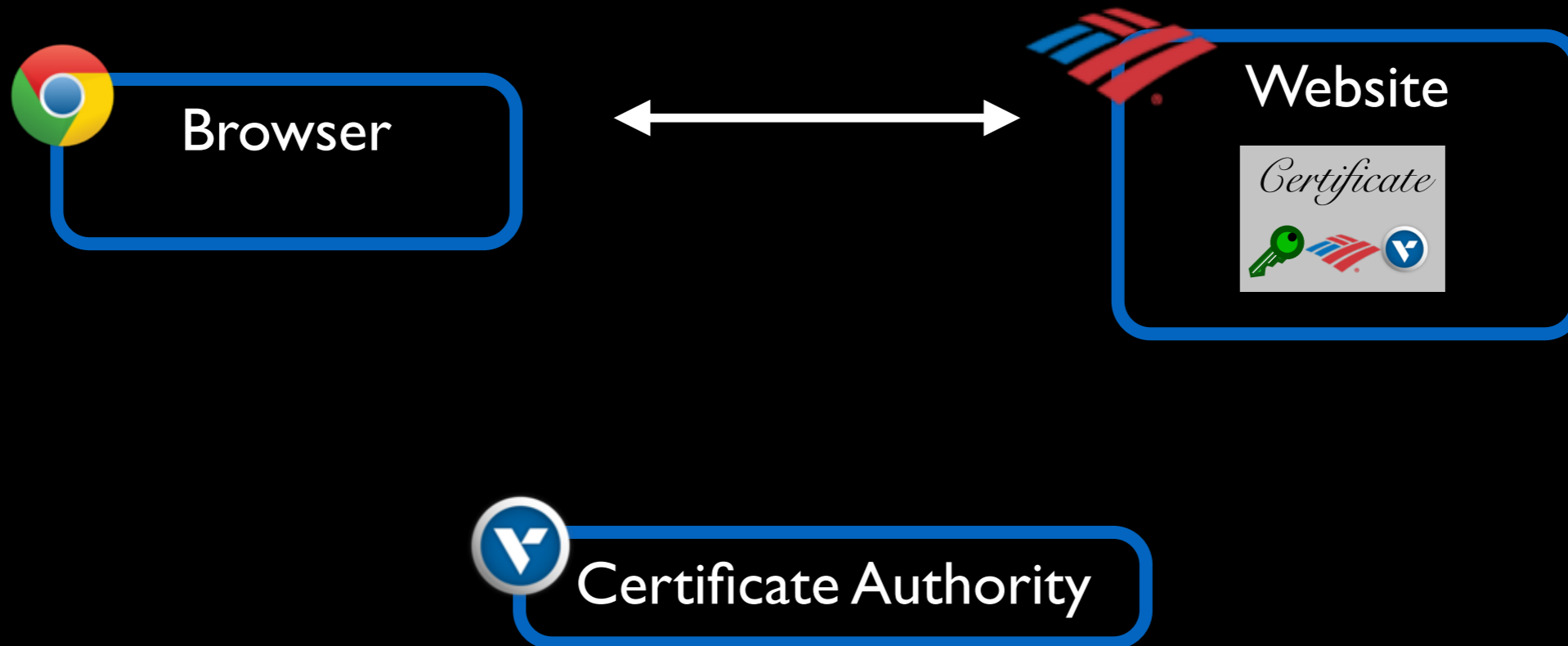


Certificate authorities behavior
e.g., **high cost in distributing revocation info**

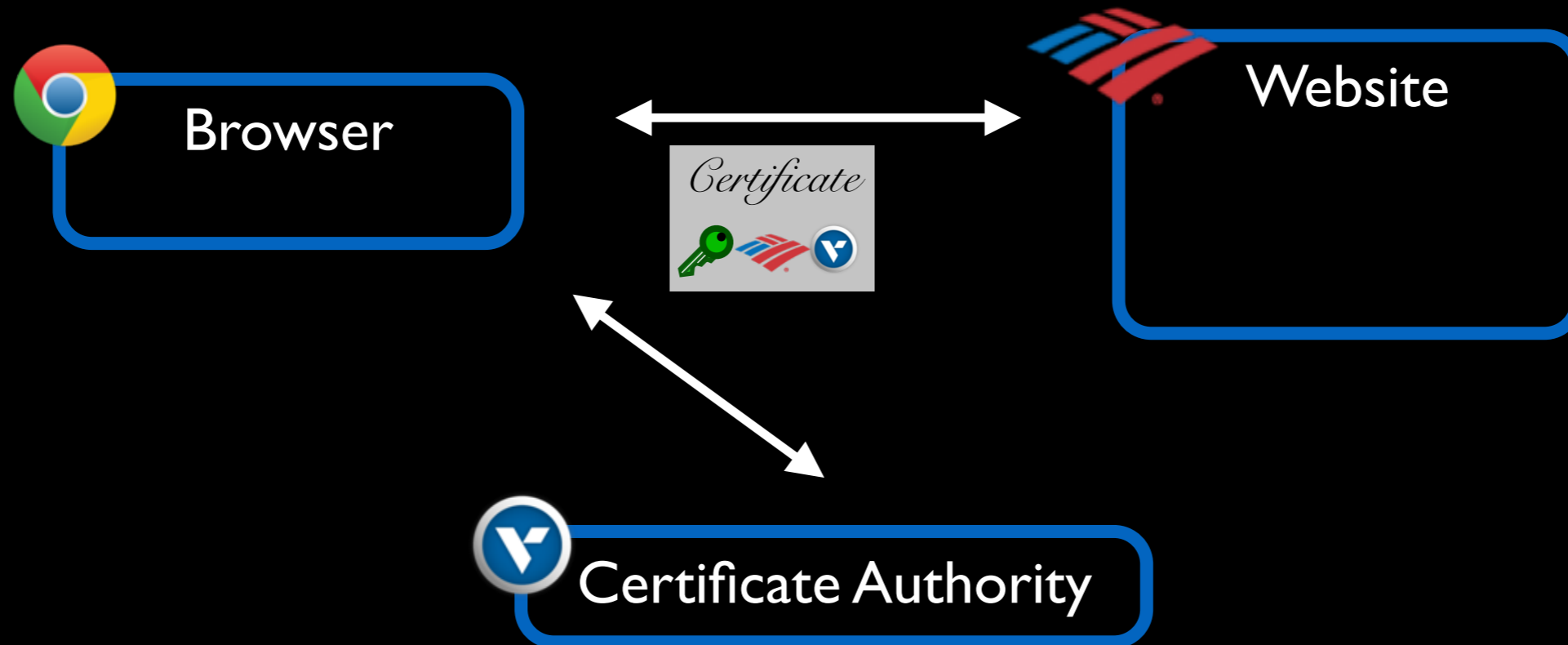


Client behavior
e.g., **do browsers check revocations?**

Security vs speed in browsers



Security vs speed in browsers



On the web, latency is king

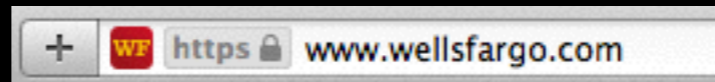
Browsers face **tension between security and speed**
Must contact CA to ensure cert not revoked

Test harness

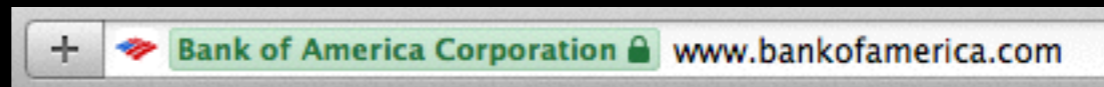
Goal: **Test browser behavior** under different combinations of:

- Revocation protocols
- Availability of revocation information
- Chain lengths
- EV/non-EV certificates

Normal



Extended Validation



Implement 244 tests using **fake root certificate + Javascript**

- Unique DNS name, cert chain, CRL/OCSP responder, ...

Do browsers check revocation info?

		Desktop Browsers									Mobile Browsers				
		Chrome 44			Firefox	Opera		Safari	IE		iOS	Andr. 4.1–5.1		IE	
		OS X	Win.	Lin.	40	12.17	31.0	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	✓	✗	✗	✗	✗
Reject unknown status		✗	✗	–	✓	✓	✗	✗	✗	✗	✗	–	–	–	–
Try CRL on failure		EV	EV	–	✗	✗	L/W	✓	✓	✓	✓	–	–	–	–
OCSP Stapling															
Request OCSP staple		✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	I	I	✗
Respect revoked staple		✗	✓	–	✓	✓	L/W	–	✓	✓	✓	–	–	–	–

Will cover few highlights...

Certificates with CRLs

		Desktop Browsers									
		Chrome 44			Firefox	Opera		Safari	IE		
		OS X	Win.	Lin.	40	12.17	31.0	6-8	7-9	10	11
CRL											
Int. 1	Revoked	EV	✓	EV	✗	✓	✓	✓	✓	✓	✓
	Unavailable	EV	✓	-	✗	✗	✓	✓	✓	✓	✓
Int. 2+	Revoked	EV	EV	EV	✗	✓	✓	✓	✓	✓	✓
	Unavailable	✗	✗	-	✗	✗	✗	✗	✗	✗	✗
Leaf	Revoked	EV	EV	EV	✗	✓	✓	✓	✓	✓	✓
	Unavailable	✗	✗	-	✗	✗	✗	✗	✗	A	✓

Chrome: Only checks CRLs for **EV certificates**

Firefox: *Never* checks CRLs

Most browsers accept certificate if **CRL server unavailable**

IE performs the most checks (!)

Certificates with OCSP

		Desktop Browsers									
		Chrome 44			Firefox	Opera		Safari	IE		
		OS X	Win.	Lin.	40	12.17	31.0	6-8	7-9	10	11
OCSP											
Int. 1	Revoked	EV	EV	EV	EV	X	✓	✓	✓	✓	✓
	Unavailable	X	X	-	X	X	L/W	X	✓	✓	✓
Int. 2+	Revoked	EV	EV	EV	EV	X	✓	✓	✓	✓	✓
	Unavailable	X	X	-	X	X	X	X	X	X	X
Leaf	Revoked	EV	EV	EV	✓	✓	✓	✓	✓	✓	✓
	Unavailable	X	X	-	X	X	X	X	X	A	✓
Reject unknown status		X	X	-	✓	✓	X	X	X	X	X
Try CRL on failure		EV	EV	-	X	X	L/W	✓	✓	✓	✓

Chrome: Only checks OCSP for EV certificates

Firefox: Only checks intermediates for EV certificates

Most browsers accept certificate if **OCSP server unavailable**

IE again performs the most checks

Web servers with OCSP Stapling

	Desktop Browsers									
	Chrome 44			Firefox	Opera		Safari	IE		
	OS X	Win.	Lin.	40	12.17	31.0	6-8	7-9	10	11
OCSP Stapling										
Request OCSP staple	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
Respect revoked staple	✗	✓	-	✓	✓	L/W	-	✓	✓	✓

All browsers support OCSP Stapling... **except Safari**

Chrome bug: accept *any* Staple on OS X, including **revoked**

What about mobile browsers?

		Mobile Browsers			
		iOS 6-8	Andr. 4.1-5.1 Stock Chrome		IE 8.0
CRL					
Int. 1	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Int. 2+	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Leaf	Revoked	X	X	X	X
	Unavailable	X	X	X	X
OCSP					
Int. 1	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Int. 2+	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Leaf	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Reject unknown status		-	-	-	-
Try CRL on failure		-	-	-	-
OCSP Stapling					
Request OCSP staple		X	I	I	X
Respect revoked staple		-	-	-	-

Mobile browsers *never* check

Android devices request Staples
...and promptly ignore them

What about mobile browsers?

		Mobile Browsers			
		iOS 6-8	Andr. 4.1-5.1 Stock Chrome	IE 8.0	
CRL					
Int. 1	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Int. 2+	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Leaf	Revoked	X	X	X	X
	Unavailable	X	X	X	X
OCSP					
Int. 1	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Int. 2+	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Leaf	Revoked	X	X	X	X
	Unavailable	X	X	X	X
Reject unknown status		-	-	-	-
Try CRL on failure		-	-	-	-
OCSP Stapling					
Request OCSP staple		X	I	I	X
Respect revoked staple		-	-	-	-

Mobile browsers *never* check

Android devices request Staples
...and promptly ignore them

No desktop or mobile browser correctly checks revocations

Takeaways

Revocations common

~1% in steady state; more than 8% after Heartbleed

Obtaining revocation information can be expensive

CRLs large, OCSP Stapling rarely supported

Many browsers don't bother to check revocation

Mobile browsers completely lack of revocation checking



Chrome pushes out curated list of revocations, called CRLSet

Limits: filtered with reason code, size limited to 250 KB, etc.



Chrome pushes out curated list of revocations, called CRLSet

Limits: filtered with reason code, size limited to 250 KB, etc.

Only 0.35% of all revocations appear in CRLSet

Only 10.5% CRLs have *any* revocations covered



Chrome pushes out curated list of revocations, called CRLSet

Limits: filtered with reason code, size limited to 250 KB, etc.

Only 0.35% of all revocations appear in CRLSet

Only 10.5% CRLs have *any* revocations covered

If we focus on revocations from popular sites (Alexa):

3.9% top 1M, 10.4% top 1K

More results in the paper

- Analysis of EV certificate revocation
 - Revoked but alive certificates
 - Speed of CRLSet updates
 - Improve CRLSets with Bloom Filters
- and more ...

Summary

- An end-to-end measurement of certificate revocation in the web
 - Covers all parties: website administrators, CAs and browsers
- Key findings
 - Extensive inaction with respect to certificate revocation
 - Browsers fails to check certificate revocation
 - Mobile browsers are lack of revocation checking
- We can improve
 - CAs can maintain more small CRLs
 - Website admins can deploy OCSP stapling

Summary

- An end-to-end measurement of certificate revocation in the web
 - Covers all parties: website administrators, CAs and browsers
- Key findings
 - Extensive inaction with respect to certificate revocation
 - Browsers fails to check certificate revocation
 - Mobile browsers are lack of revocation checking
- We can improve
 - CAs can maintain more small CRLs
 - Website admins can deploy OCSP stapling

Questions?

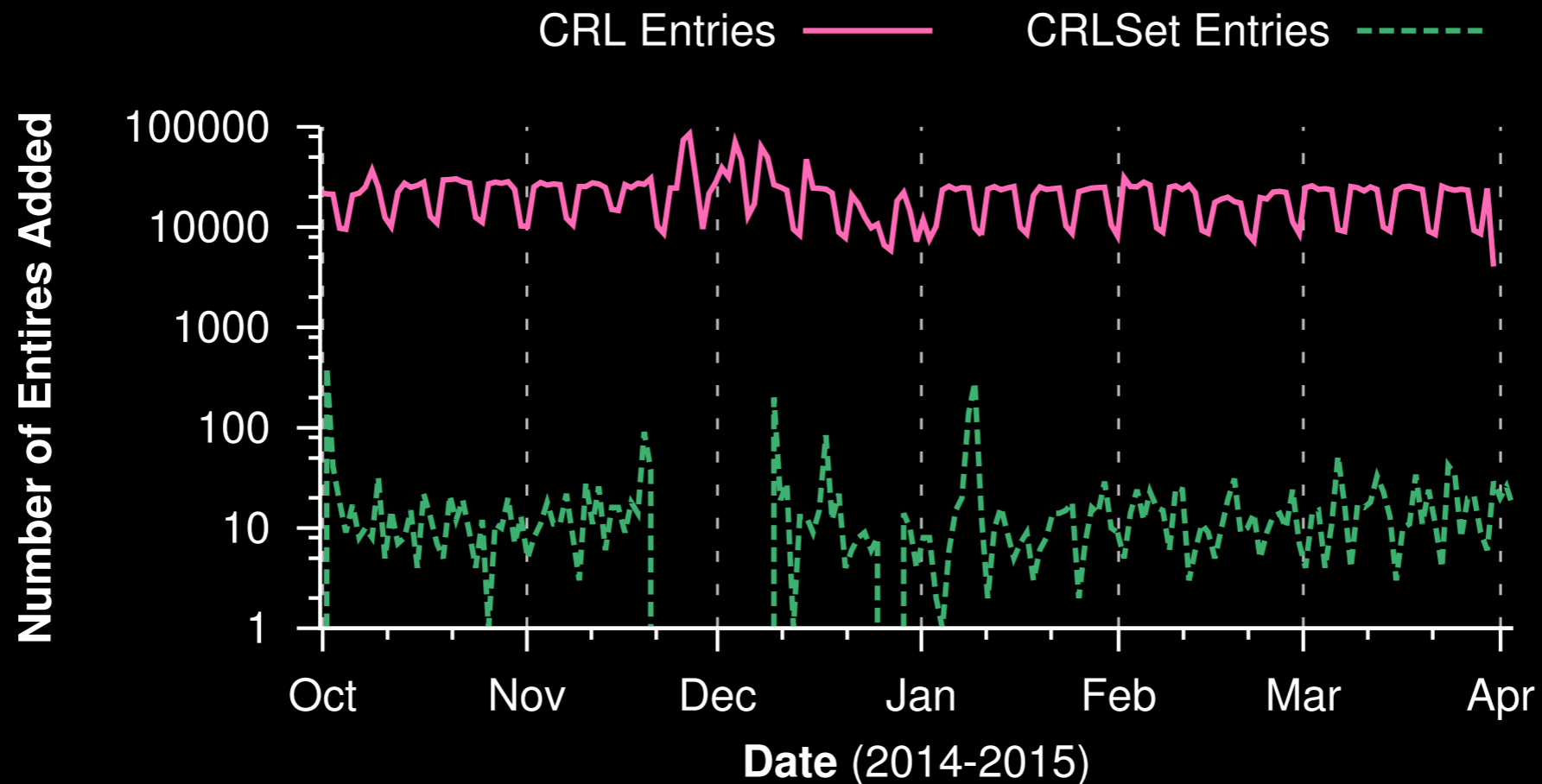
securepki.org

Backup Slides

CRLSet coverage

Only 0.35% of all revocations appear in CRLSet

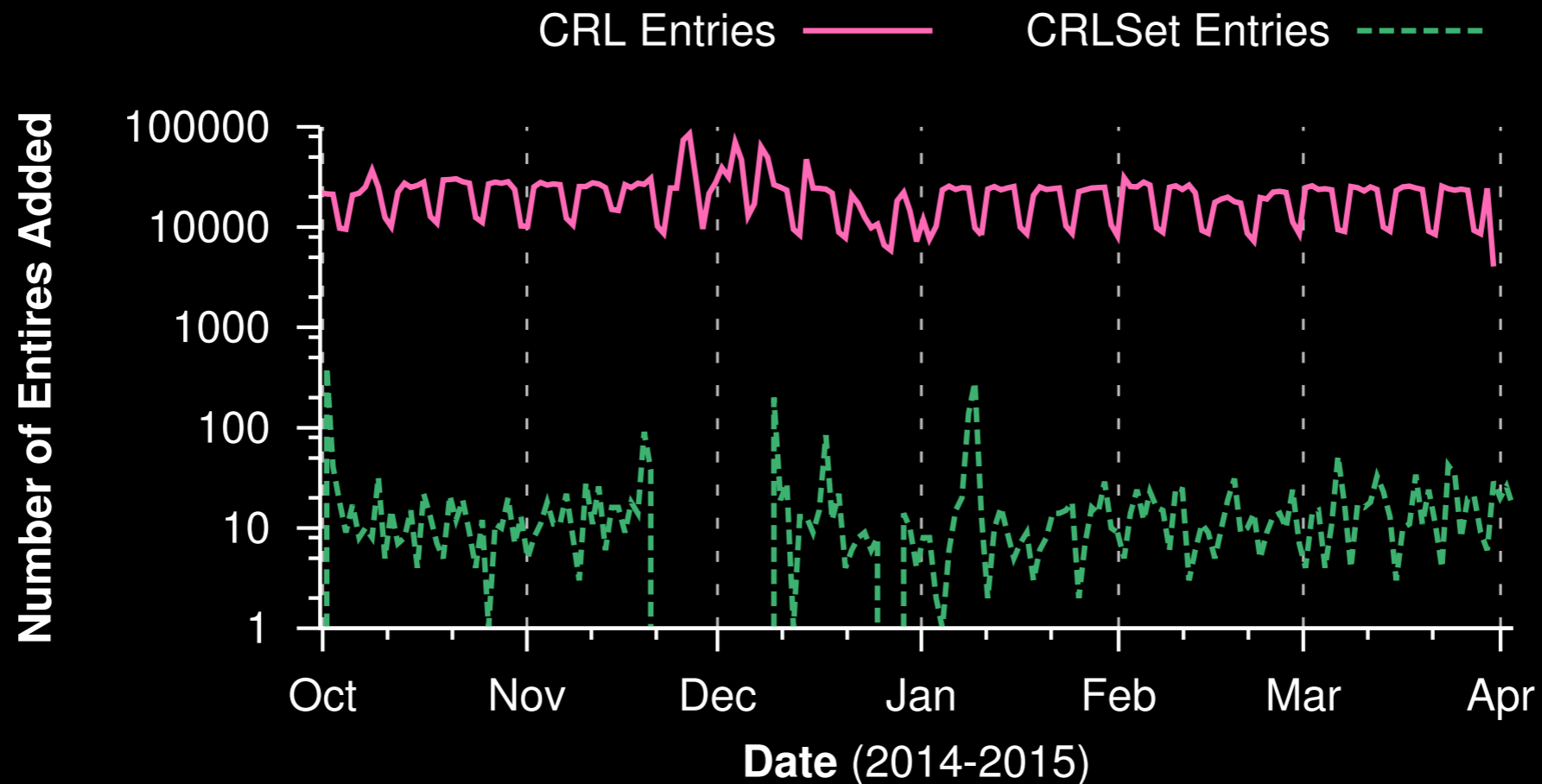
Only 295 (10.5%) CRLs have *any* revocations covered



CRLSet coverage

Only 0.35% of all revocations appear in CRLSet

Only 295 (10.5%) CRLs have *any* revocations covered



CRLSet only has a low coverage

