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

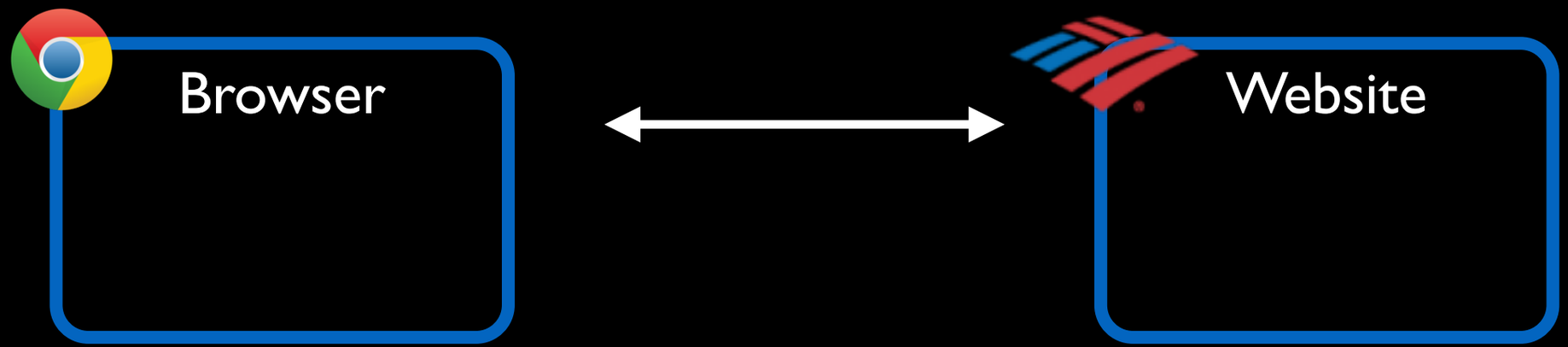
Yabing Liu*, Will Tome*, Liang Zhang*, David Choffnes*, Dave Levin†, Bruce Maggs‡, Alan Mislove*, Aaron Schulman§, Christo Wilson*

*Northeastern University †University of Maryland

‡Duke University and Akamai Technologies §Stanford University

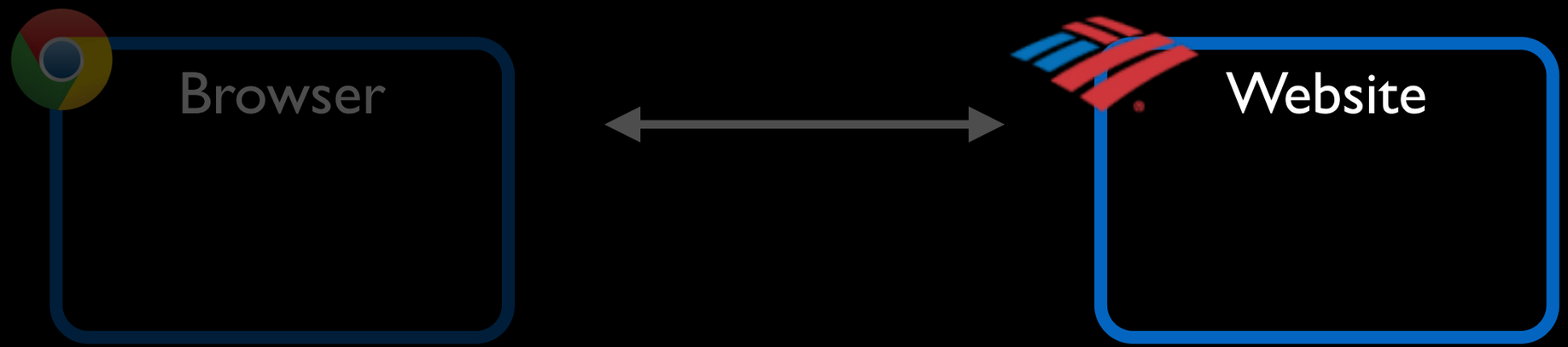
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



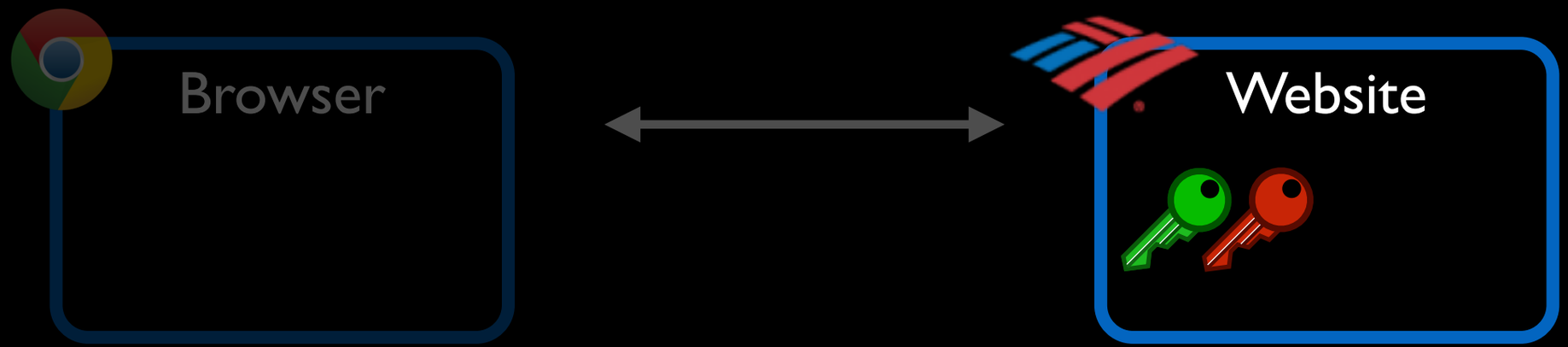
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



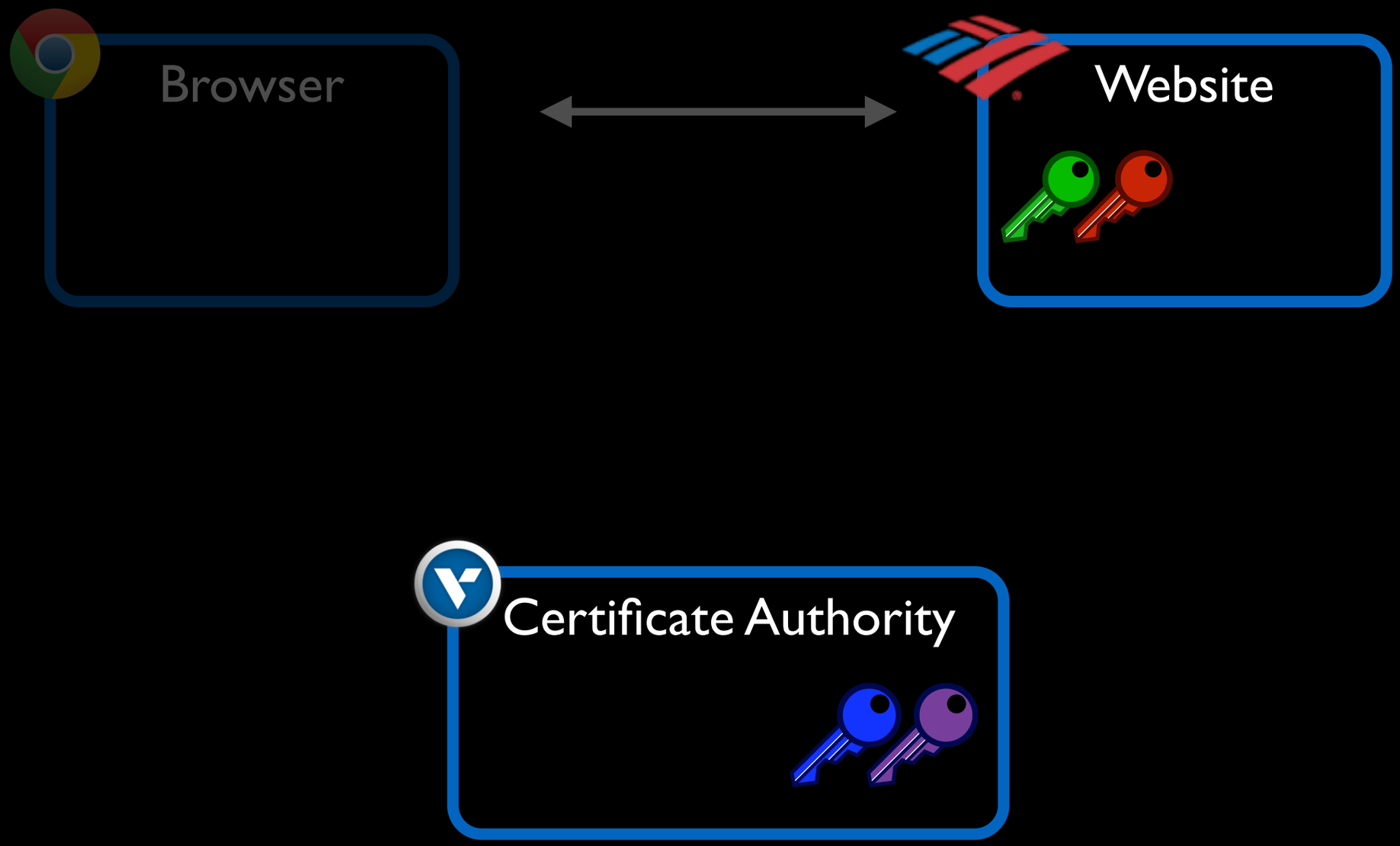
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



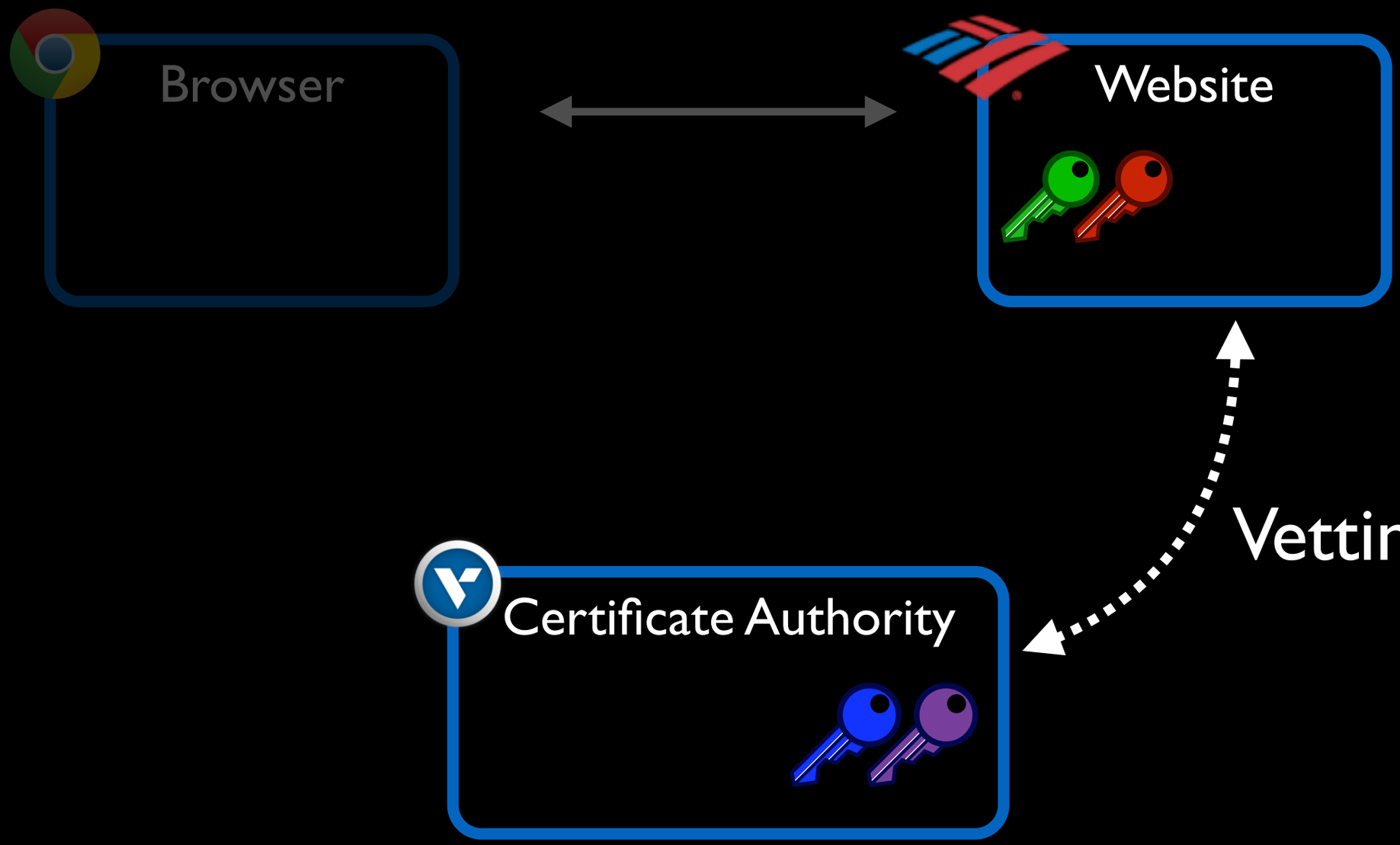
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



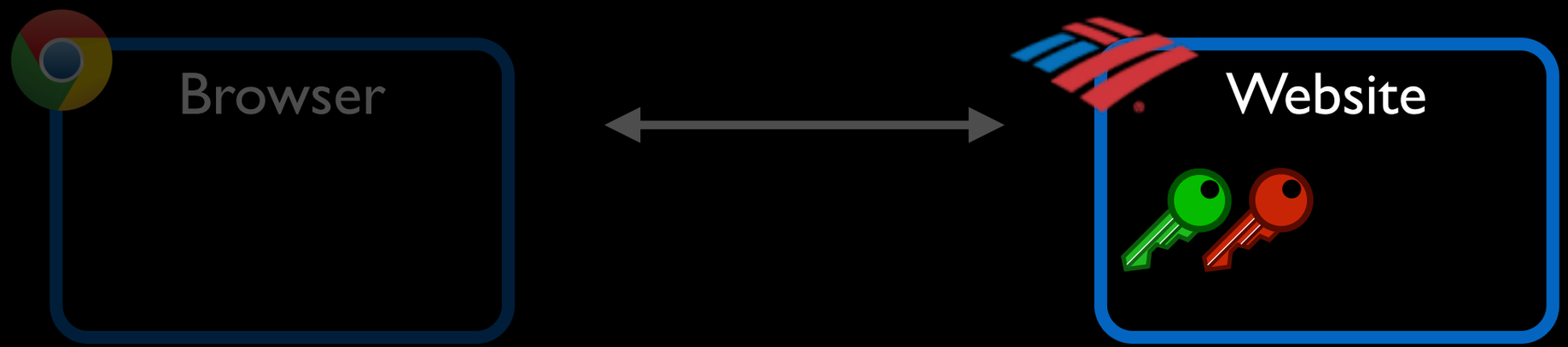
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



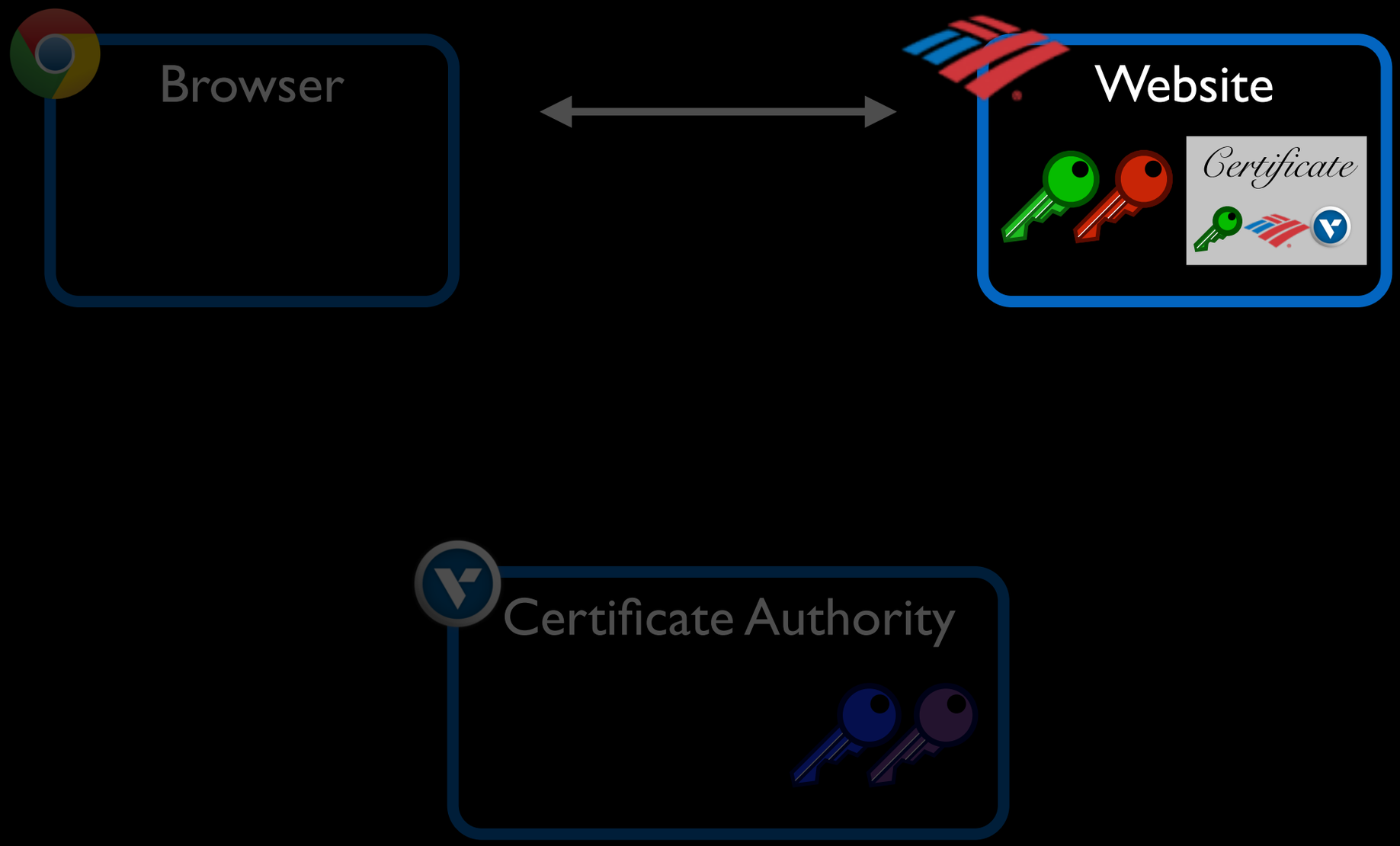
Certificate

Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?

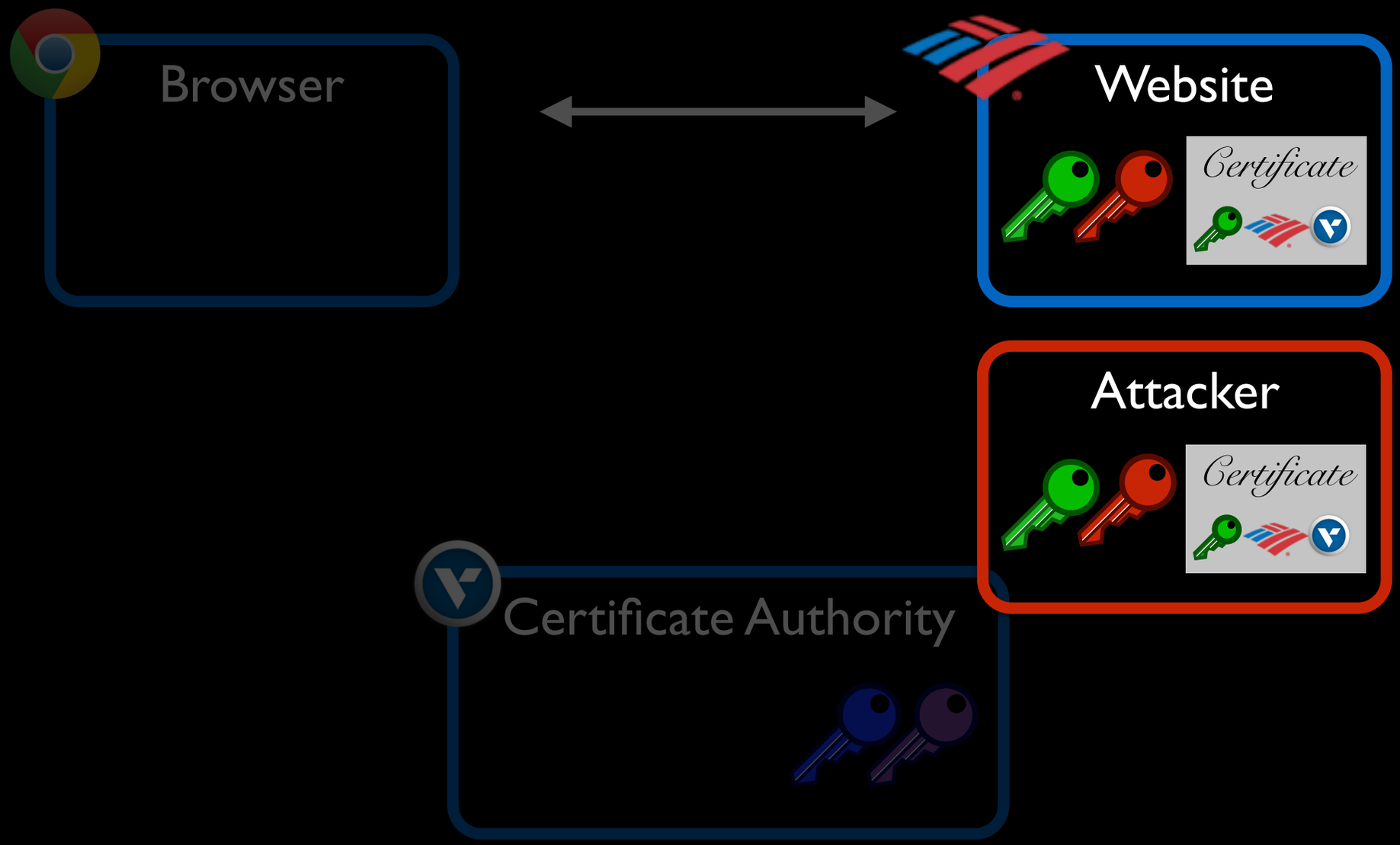
Certificate revocation

What happens when a certificate is no longer valid?



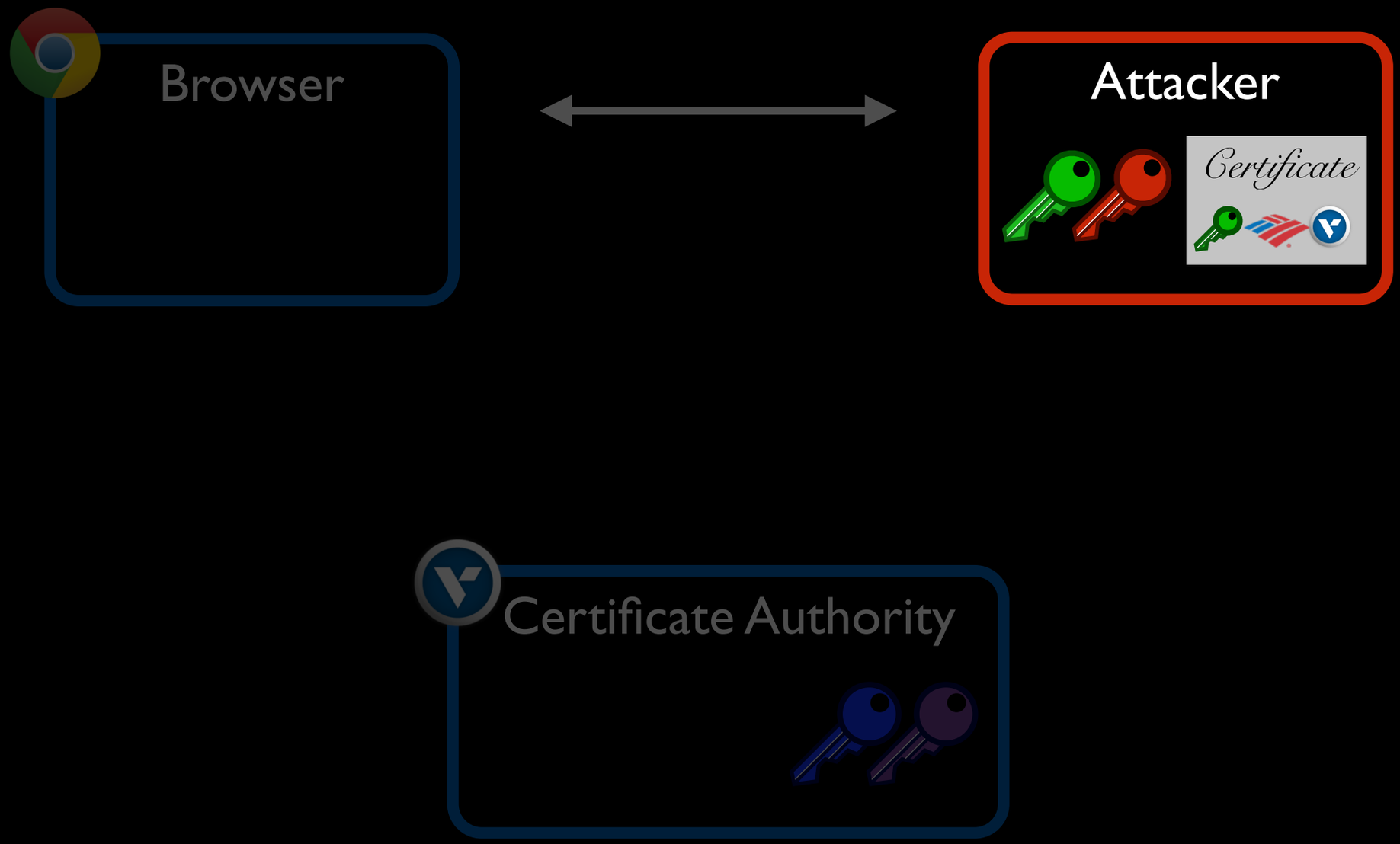
Certificate revocation

What happens when a certificate is no longer valid?



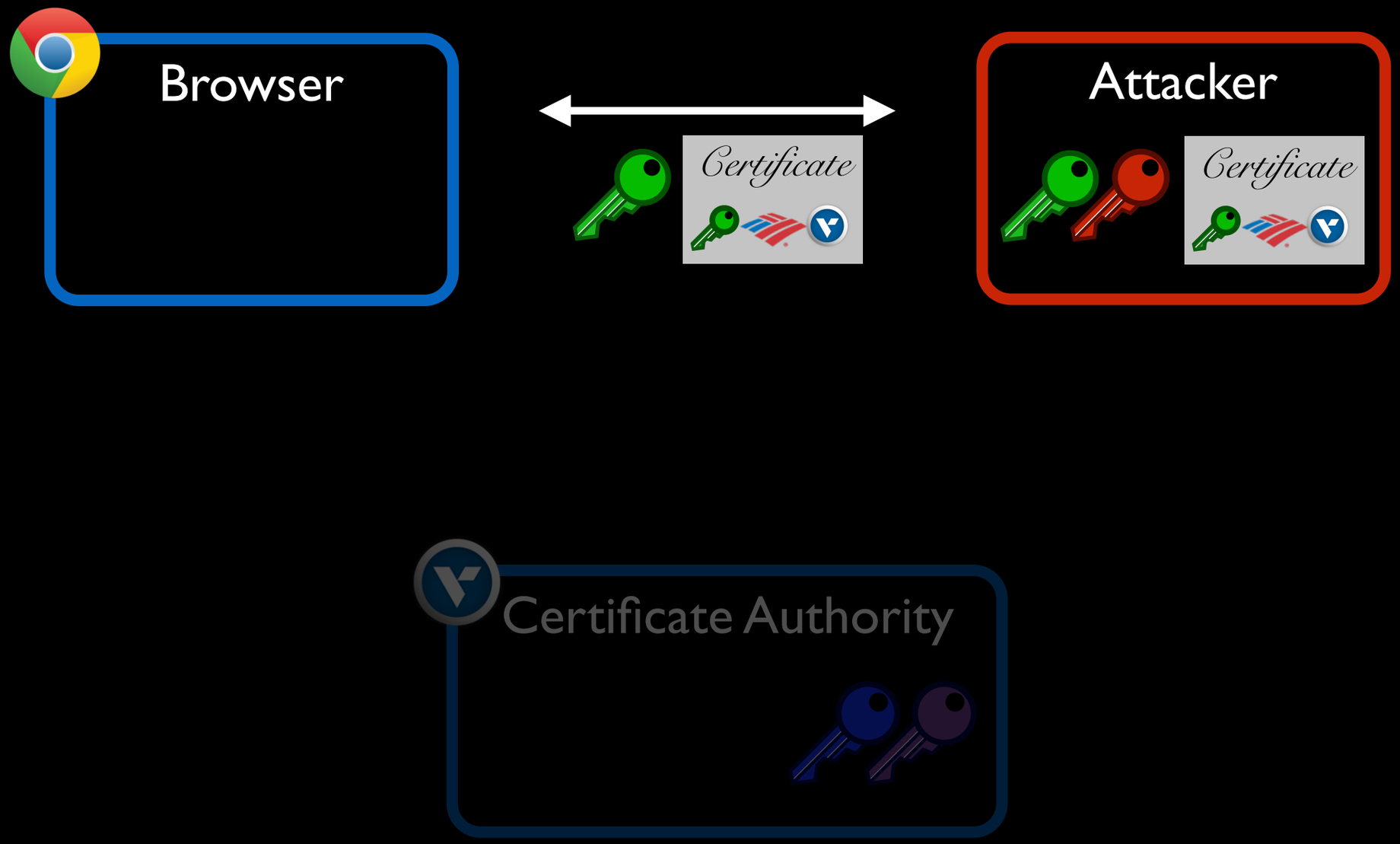
Certificate revocation

What happens when a certificate is no longer valid?



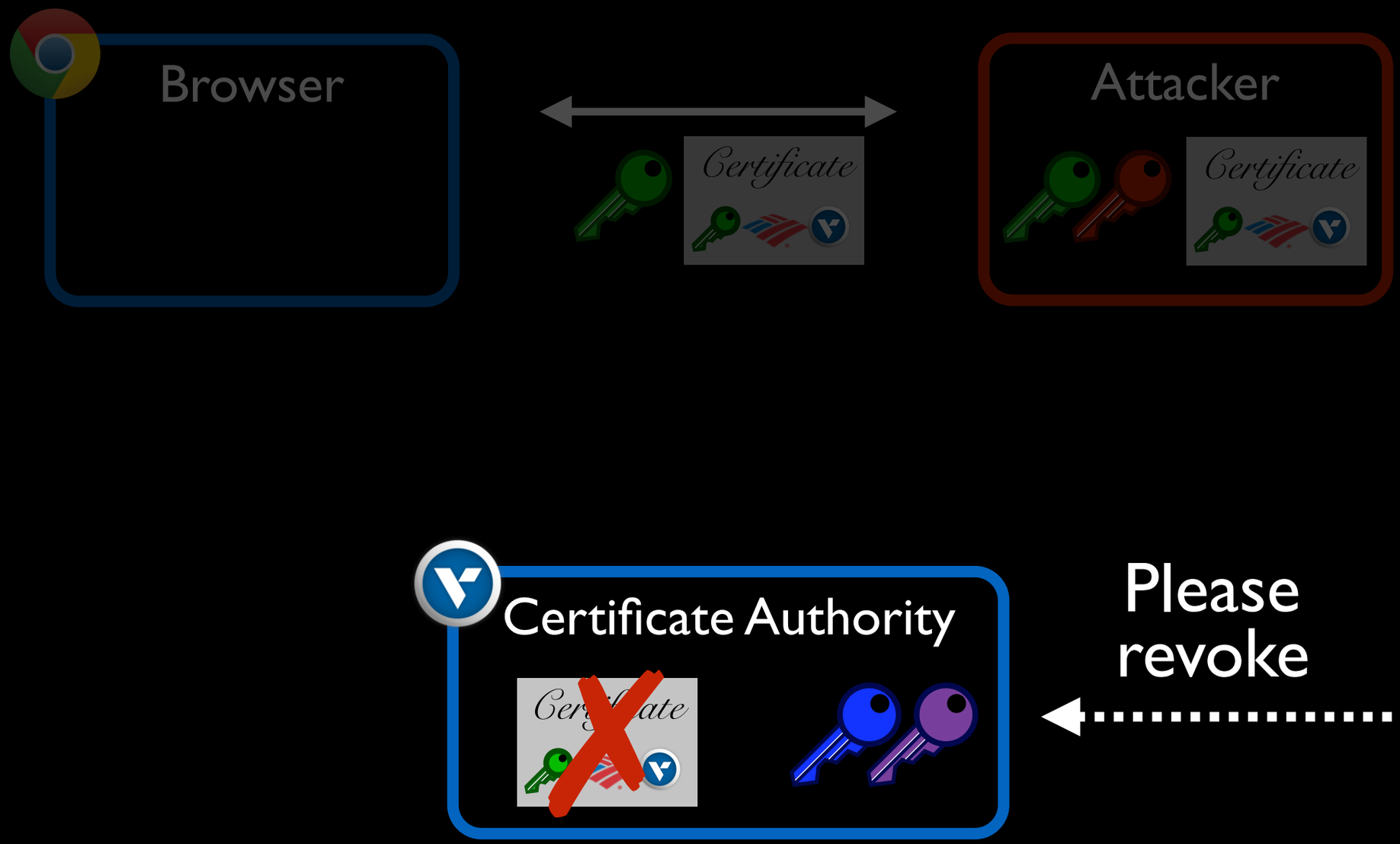
Certificate revocation

What happens when a certificate is no longer valid?



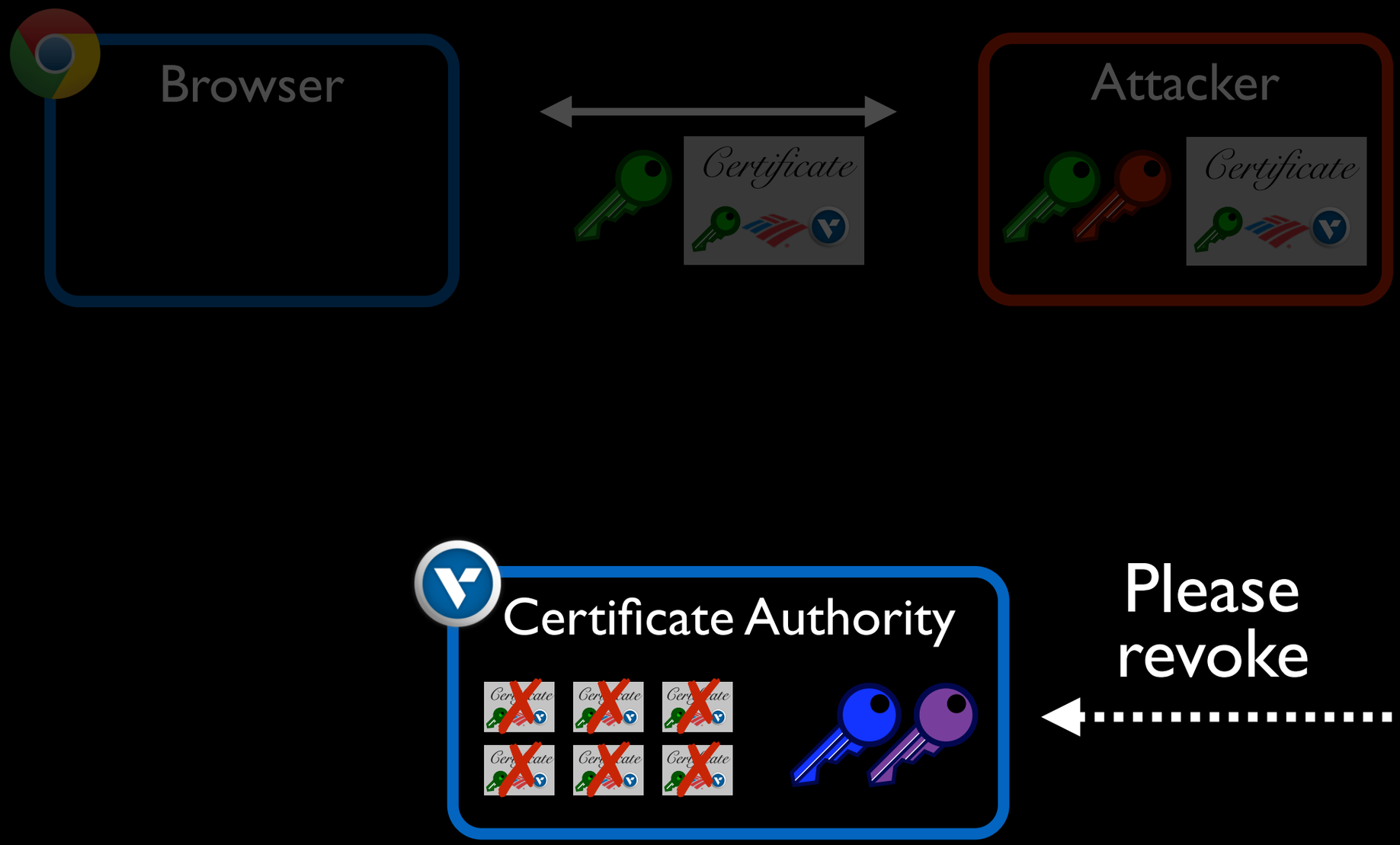
Certificate revocation

What happens when a certificate is no longer valid?



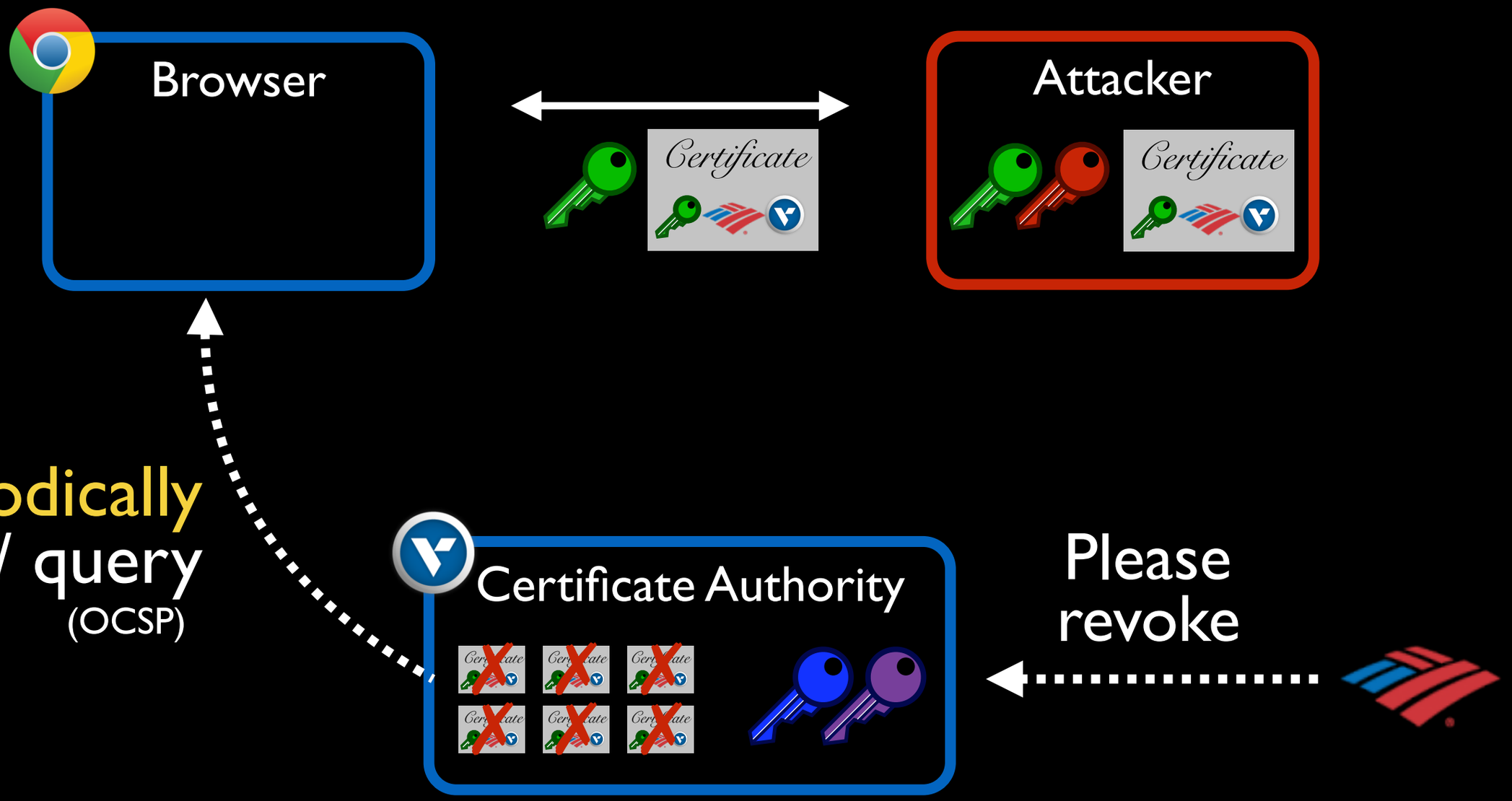
Certificate revocation

What happens when a certificate is no longer valid?



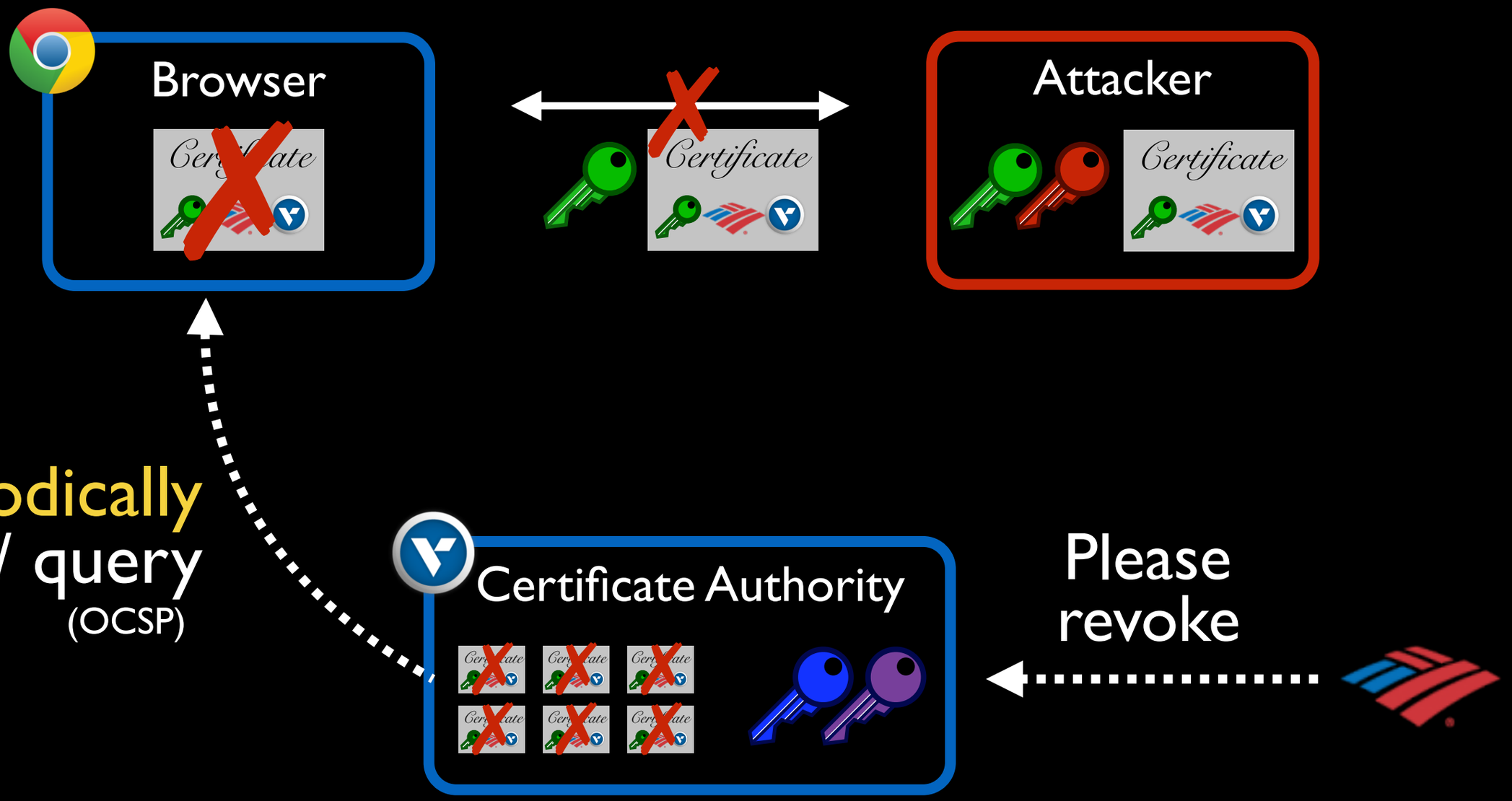
Certificate revocation

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 CAs serve revocations?

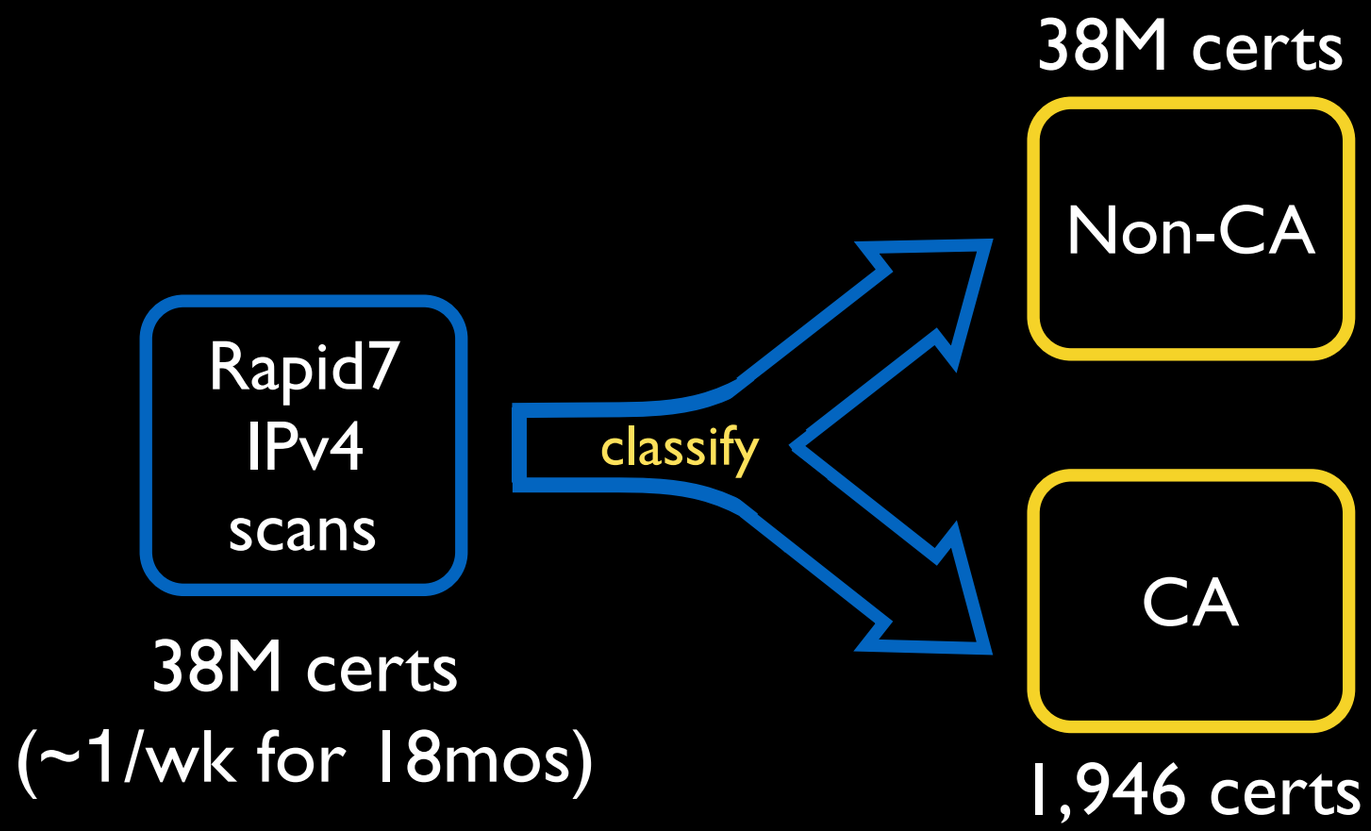
Client behavior
e.g., do browsers check revocations?

Dataset

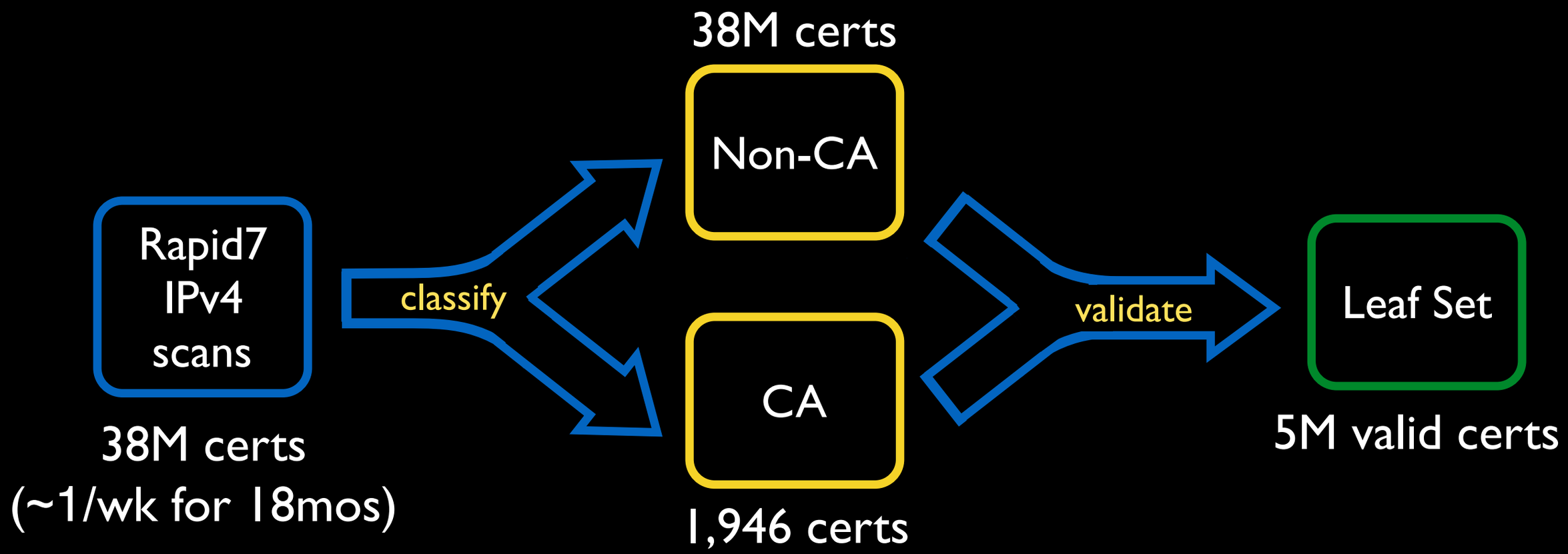
Rapid7
IPv4
scans

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

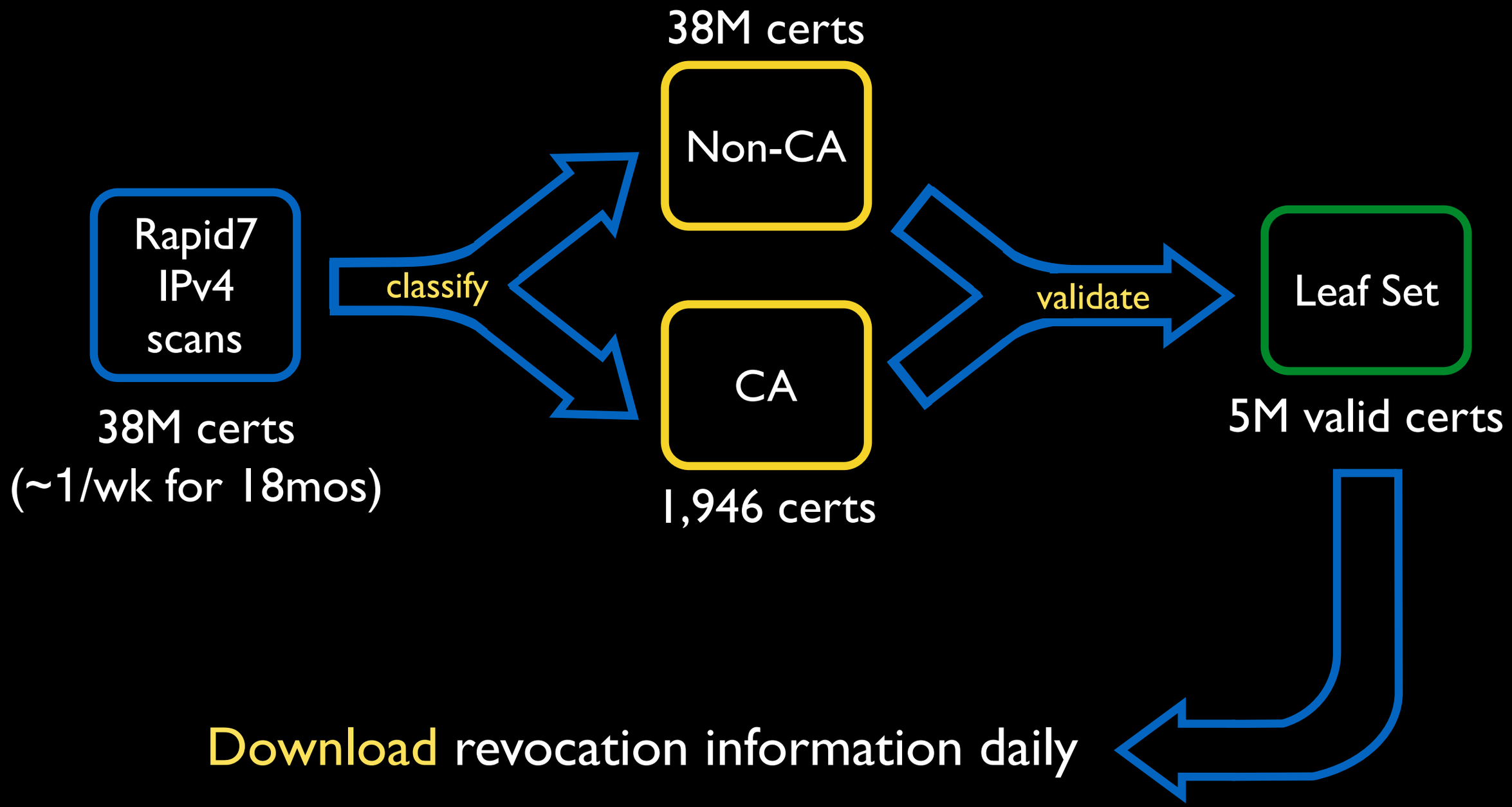
Dataset


38M certs
Non-CA
Rapid7
IPv4
scans
classify
CA
38M certs
(~1/wk for 18mos)
1,946 certs

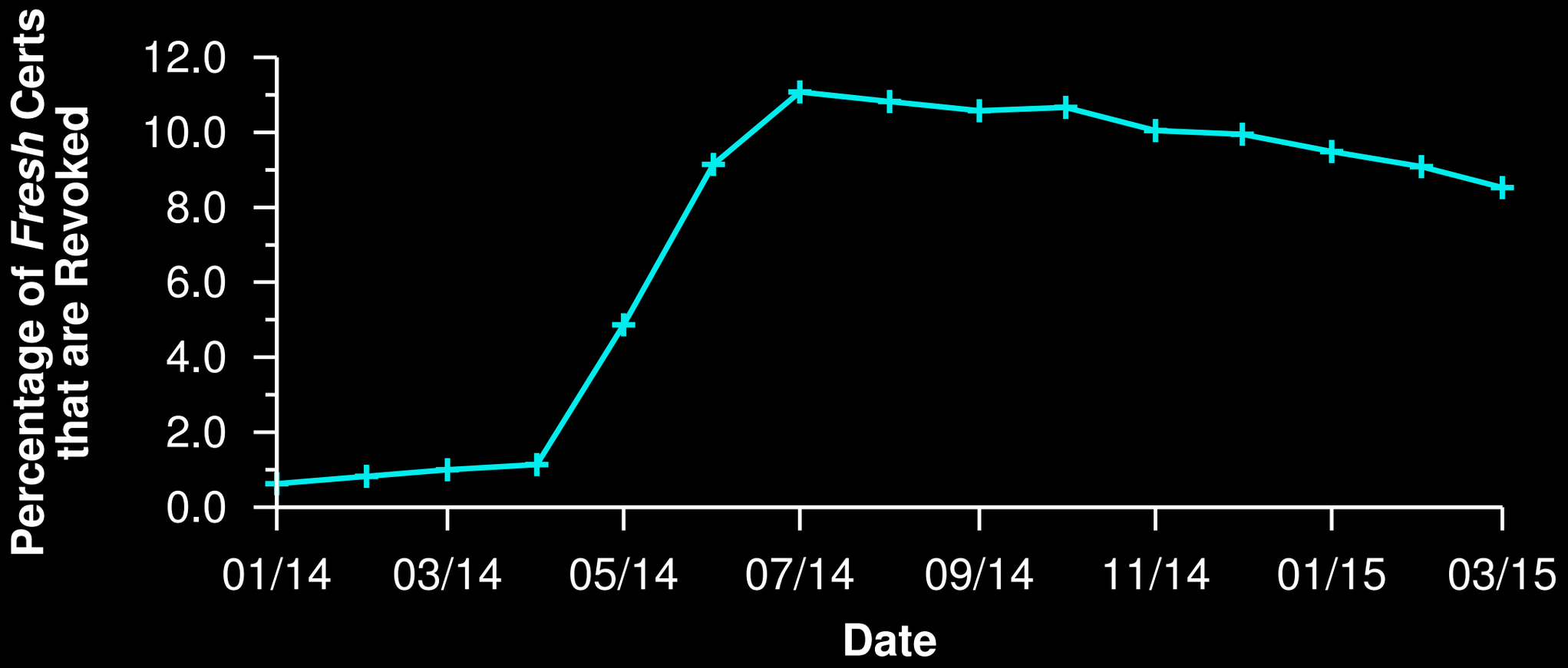
Dataset


38M certs
Non-CA
Rapid7
IPv4
scans
classify
CA
validate
Leaf Set
38M certs
(~1/wk for 18mos)
1,946 certs
5M valid certs

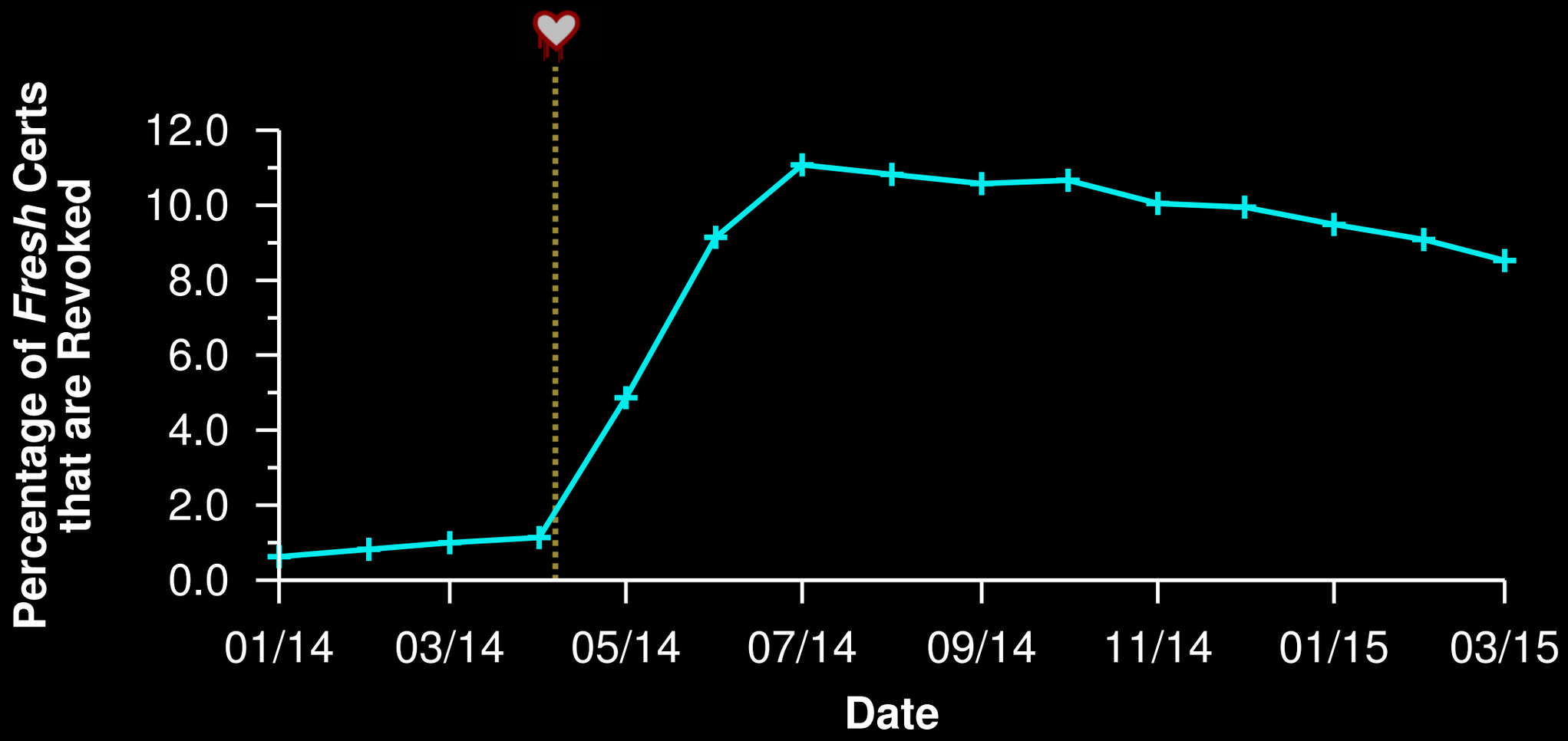
Dataset


38M certs
Non-CA
Rapid7
IPv4
scans
classify
validate
Leaf Set
CA
38M certs
(~1/wk for 18mos)
1,946 certs
5M valid certs
Download revocation information daily

How frequently are certificates revoked?



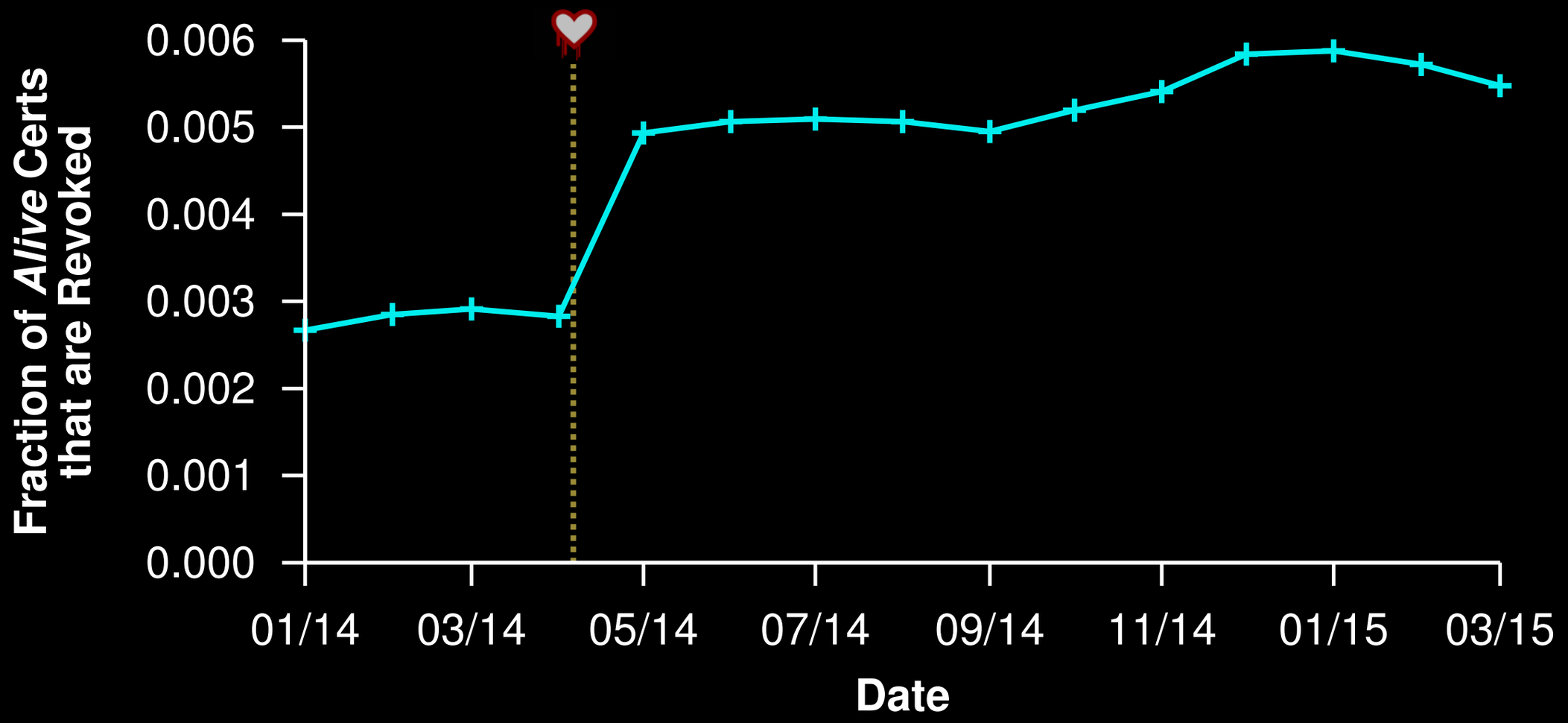
How frequently are certificates revoked?



Significant fraction of certificates revoked

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

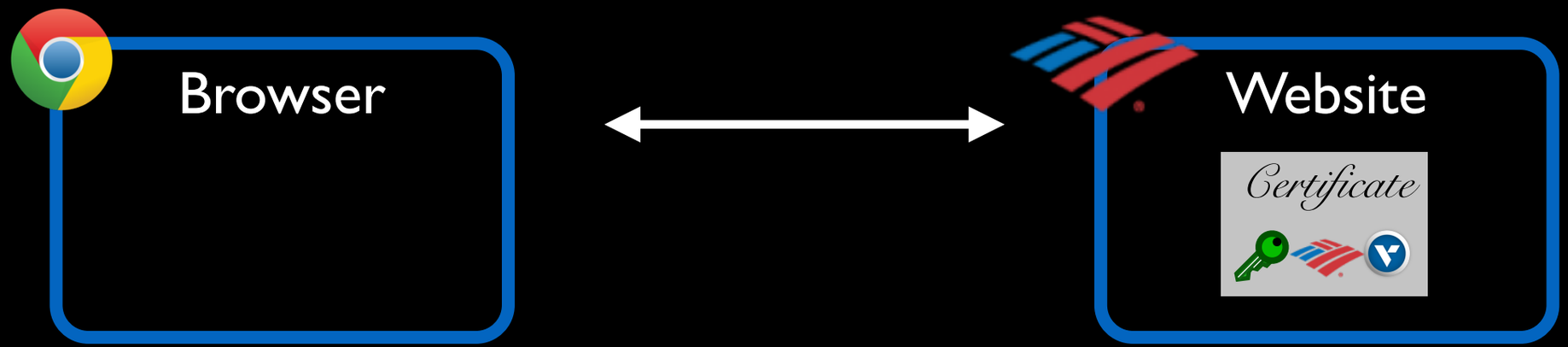
How frequently are certificates revoked?



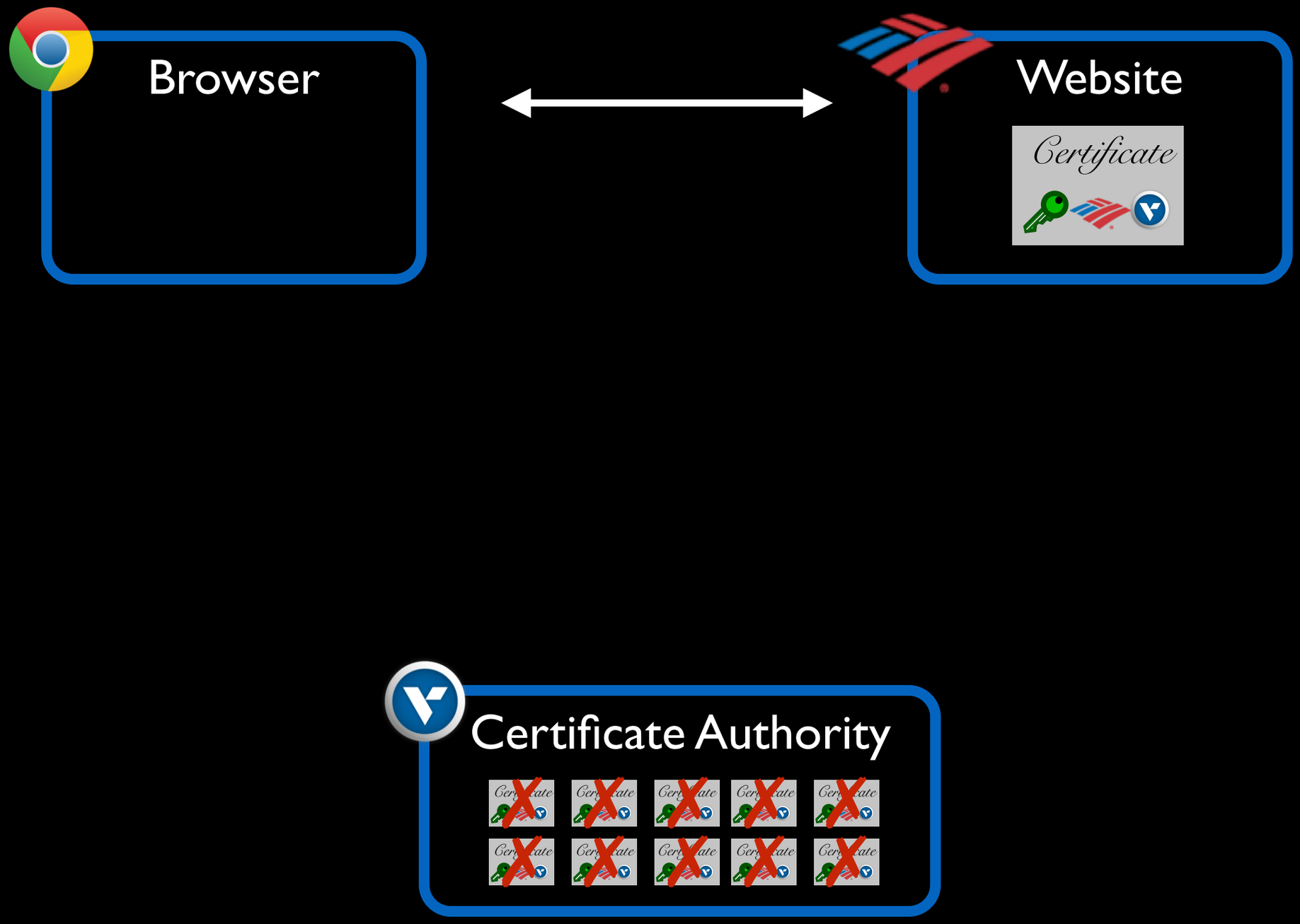
Over 0.5% advertised certificates are revoked

Website admins failed to update their servers

CRLs, OCSP, and OCSP Stapling

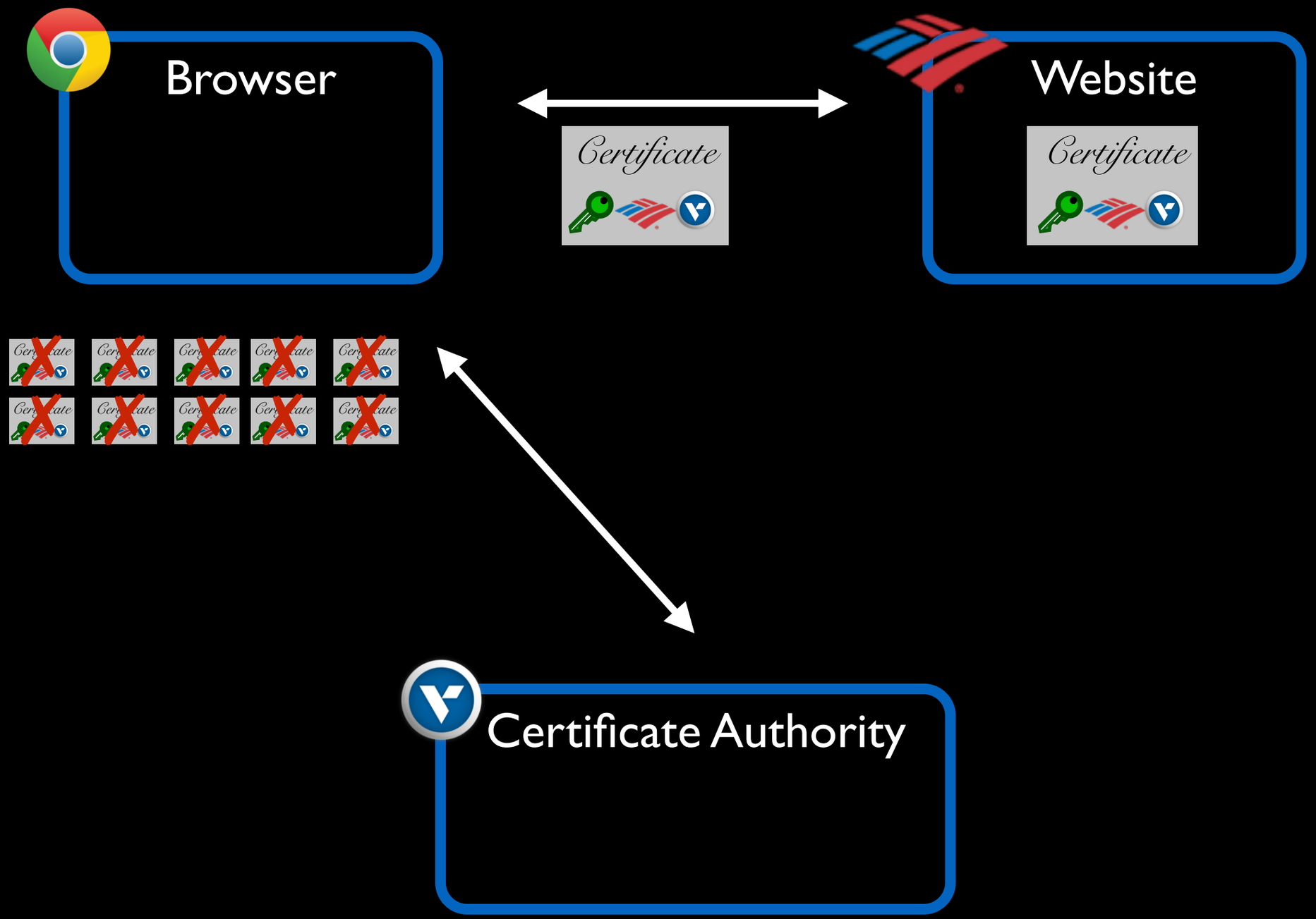


CRLs, OCSP, and OCSP Stapling

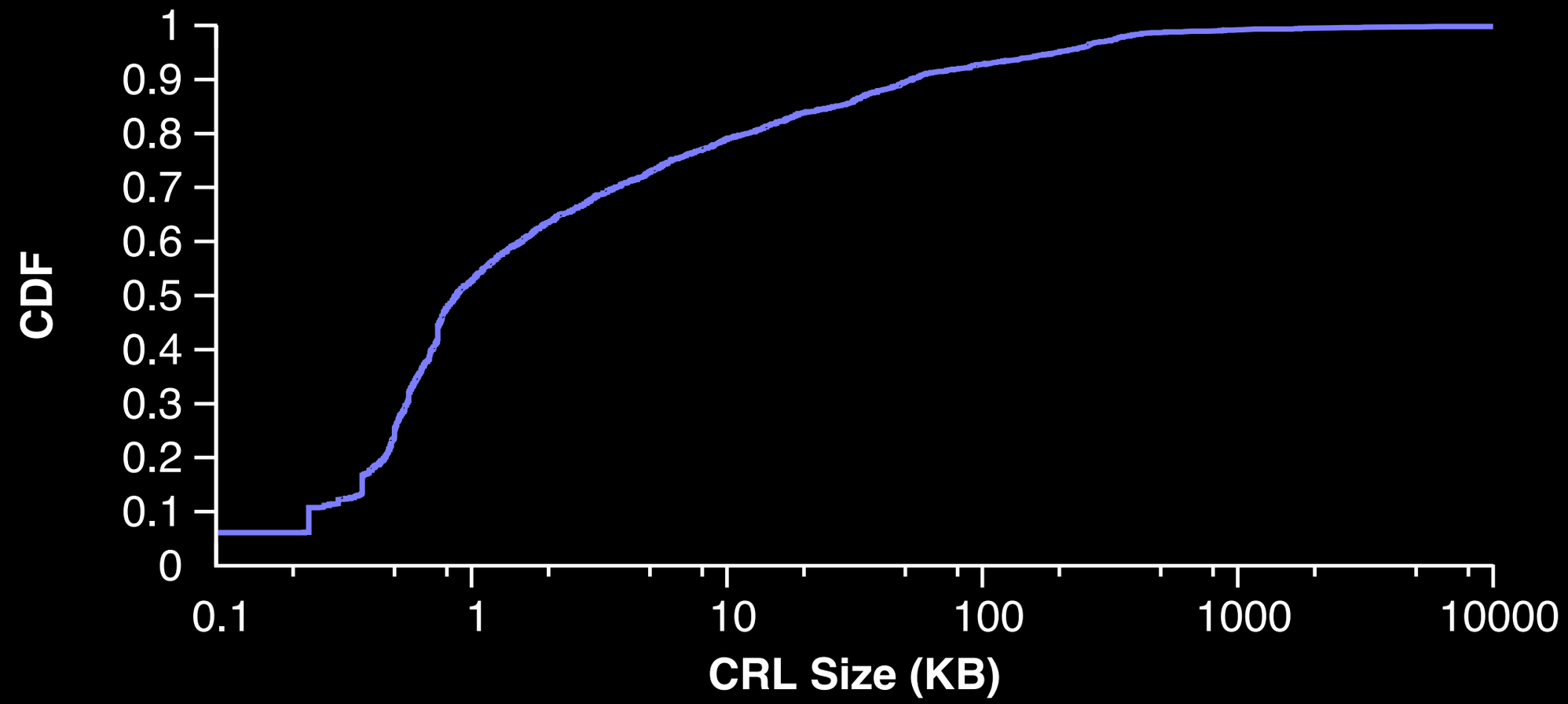


CRLs, OCSP, and OCSP Stapling

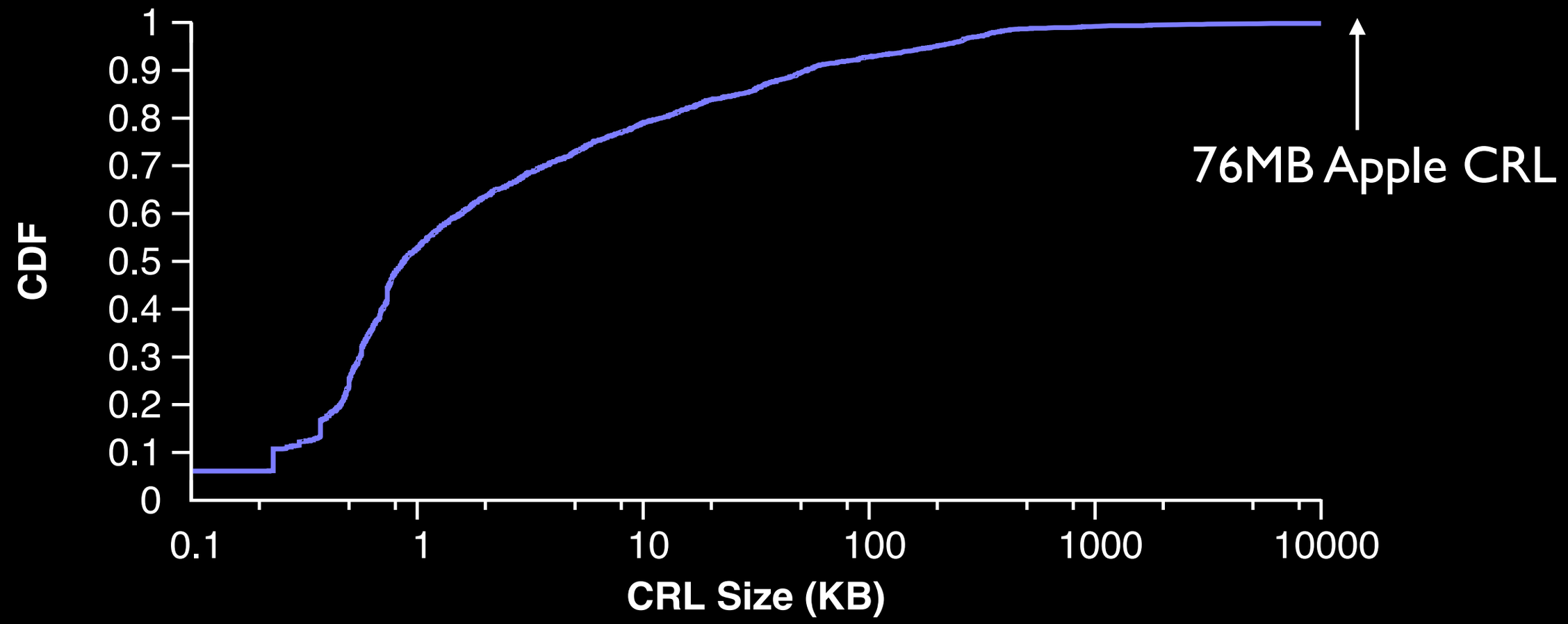
CRLs, OCSP, and OCSP Stapling



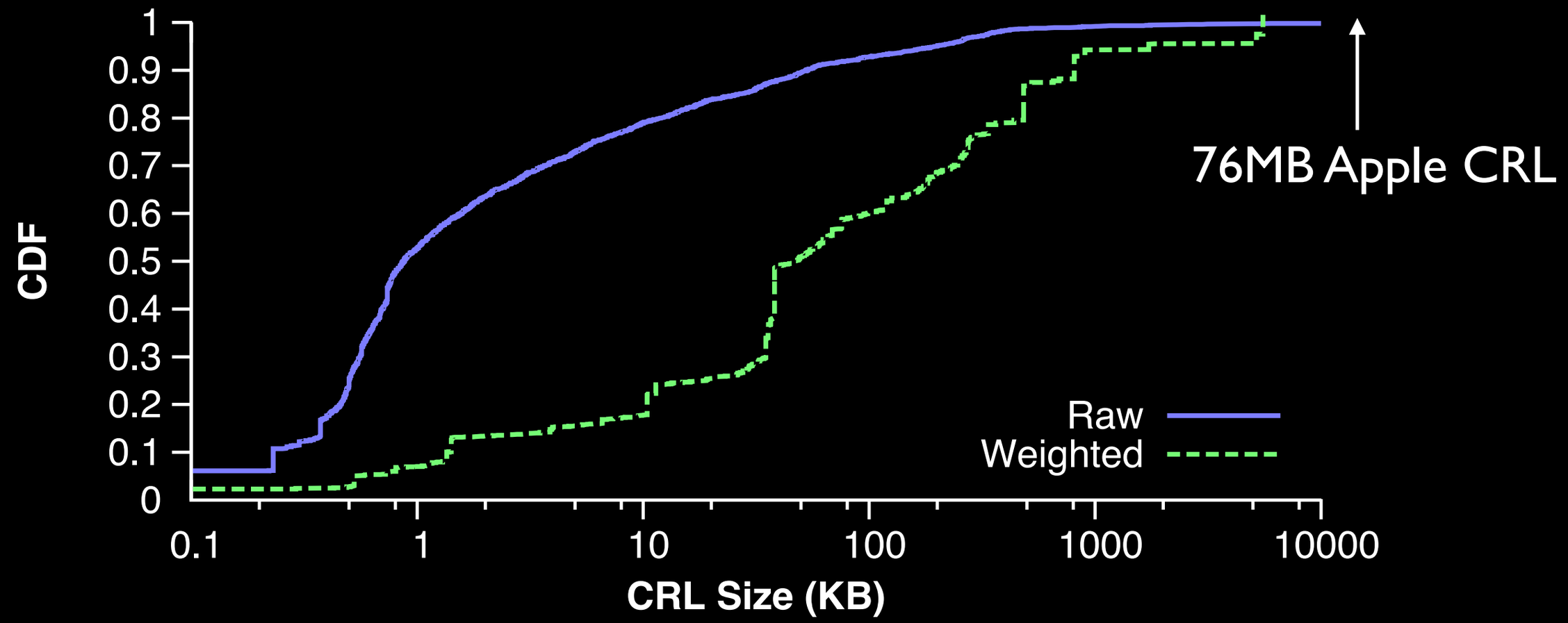
Cost of obtaining CRLs



Cost of obtaining CRLs



Cost of obtaining CRLs



Most CRLs small, but large CRLs downloaded more often

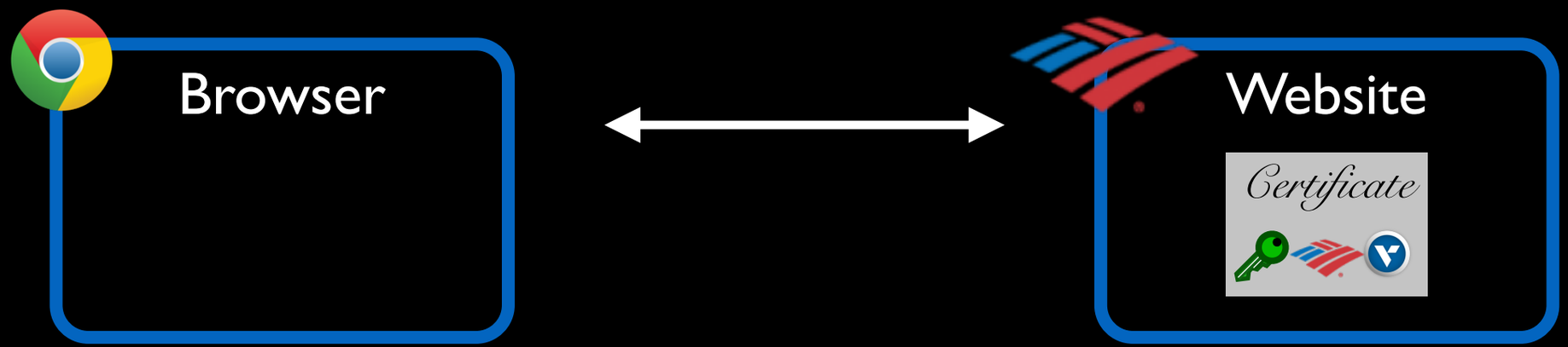
Result: 50% of certs have CRLs larger than 45KB

CRLs from different CAs

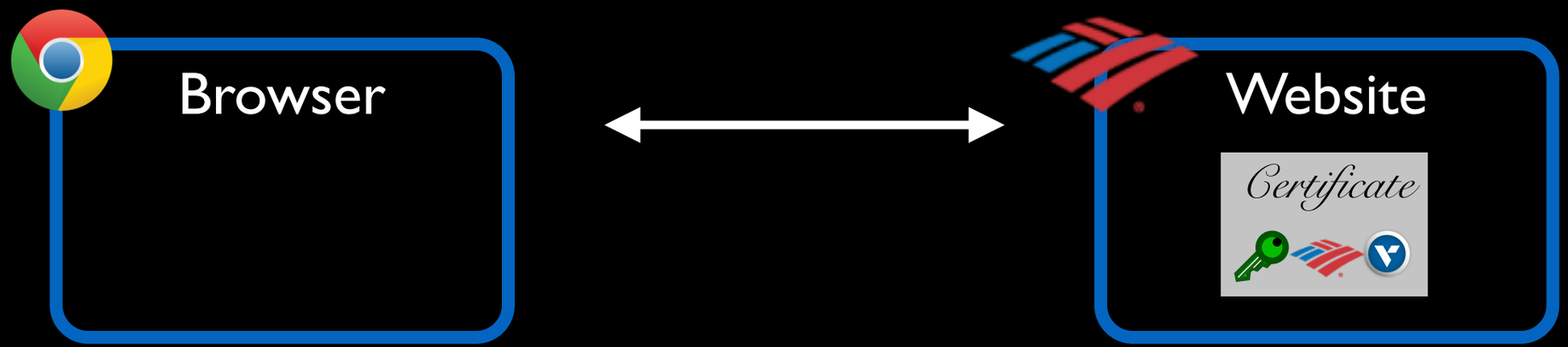
CA	Unique CRLs	Certificates		Avg. CRL size (KB)
		Total	Revoked	
GoDaddy	322	1,050,014	277,500	1,184.0
RapidSSL	5	626,774	2,153	34.5
Comodo	30	447,506	7,169	517.6
PositiveSSL	3	415,075	8,177	441.3
Verisign	37	311,788	15,438	205.2

CAs use only a small number of CRLs

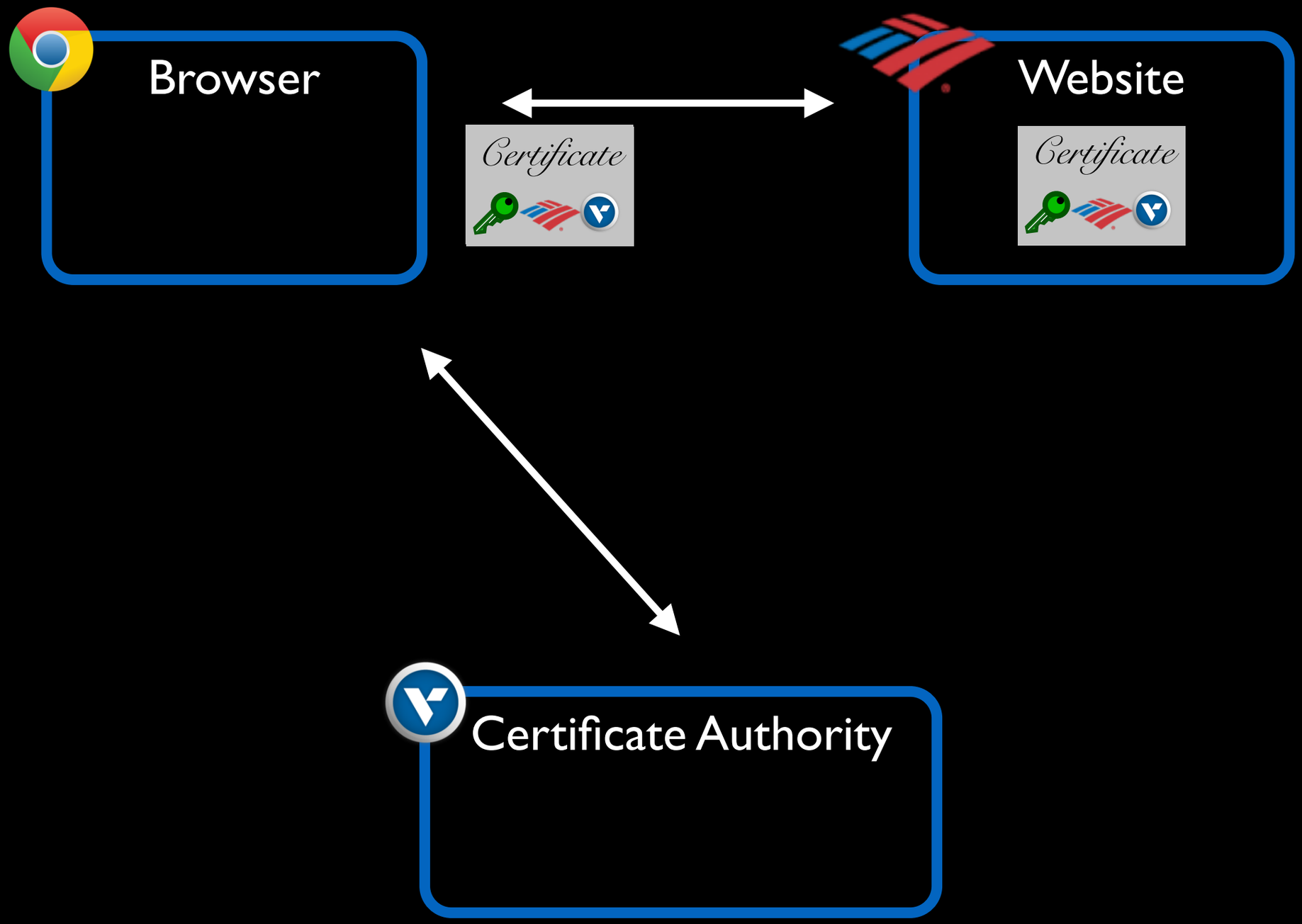
CRLs, OCSP, and OCSP Stapling



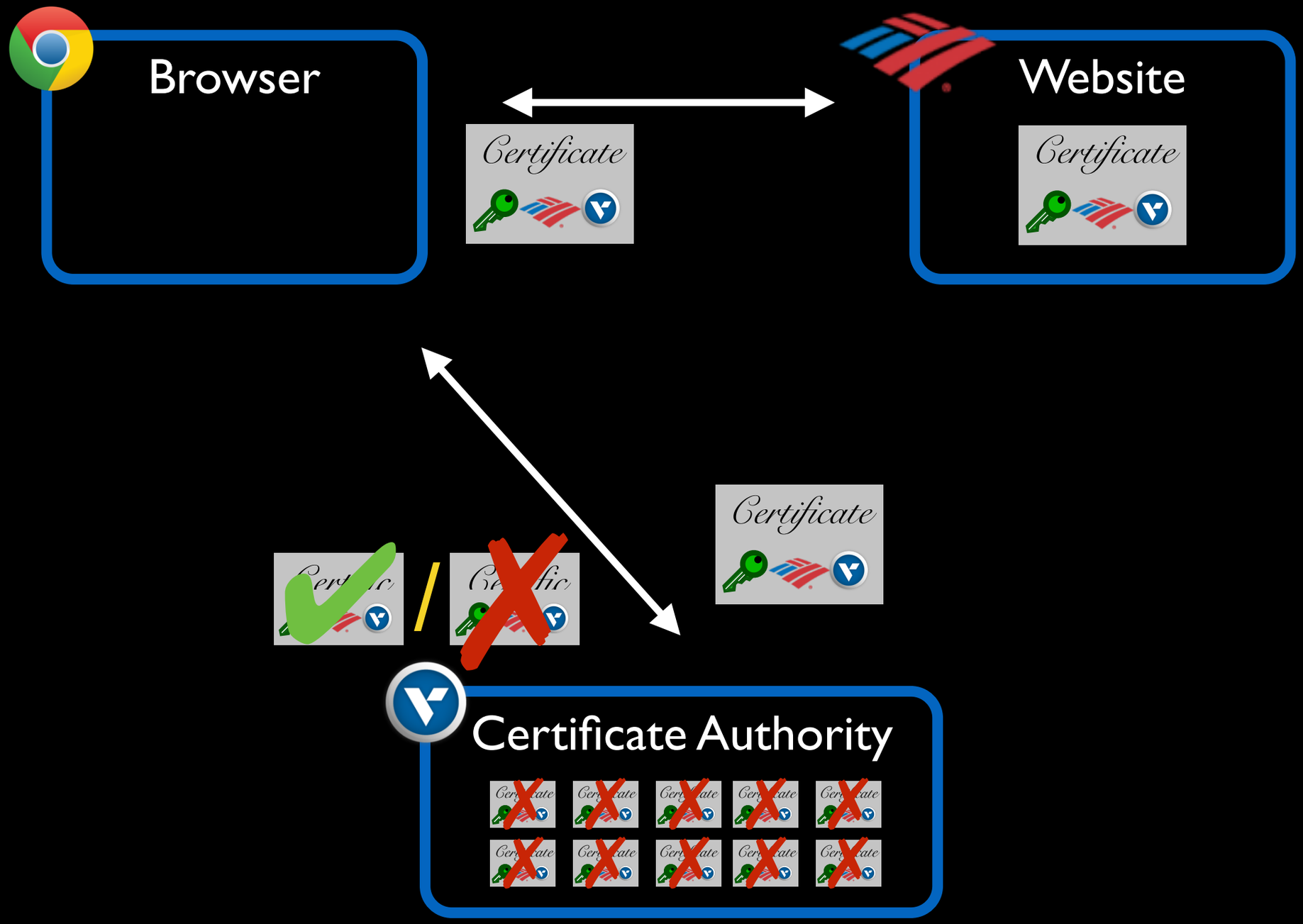
CRLs, OCSP, and OCSP Stapling



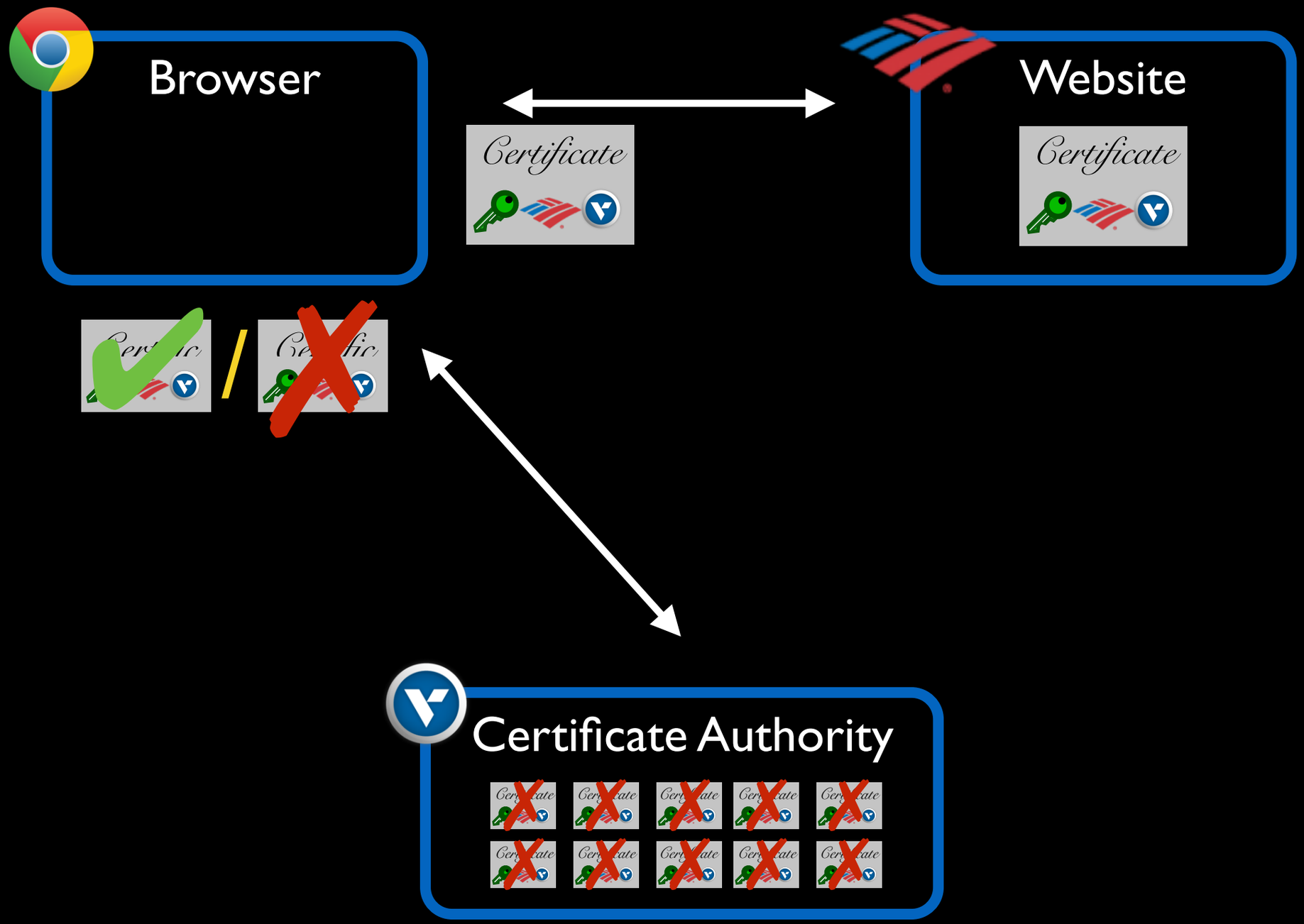
CRLs, OCSP, and OCSP Stapling



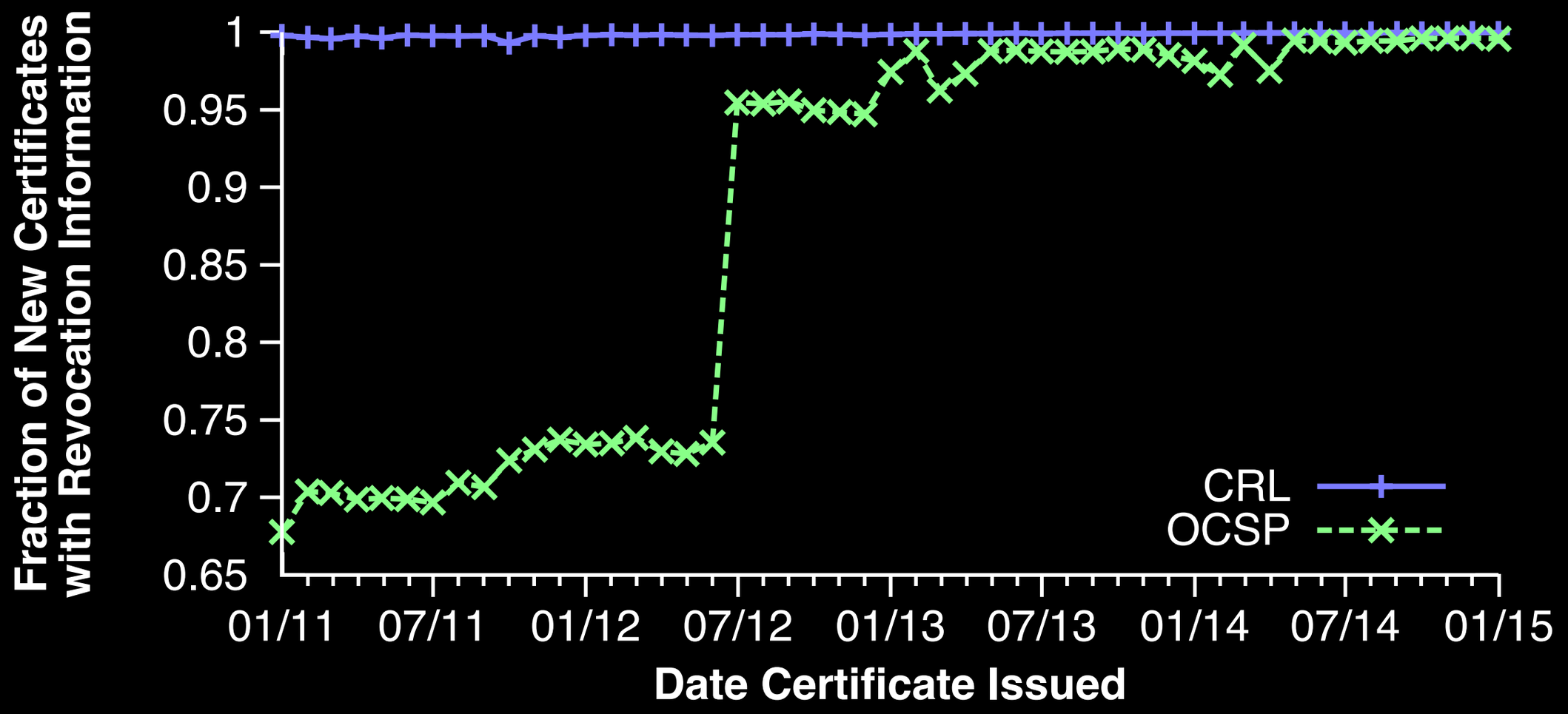
CRLs, OCSP, and OCSP Stapling



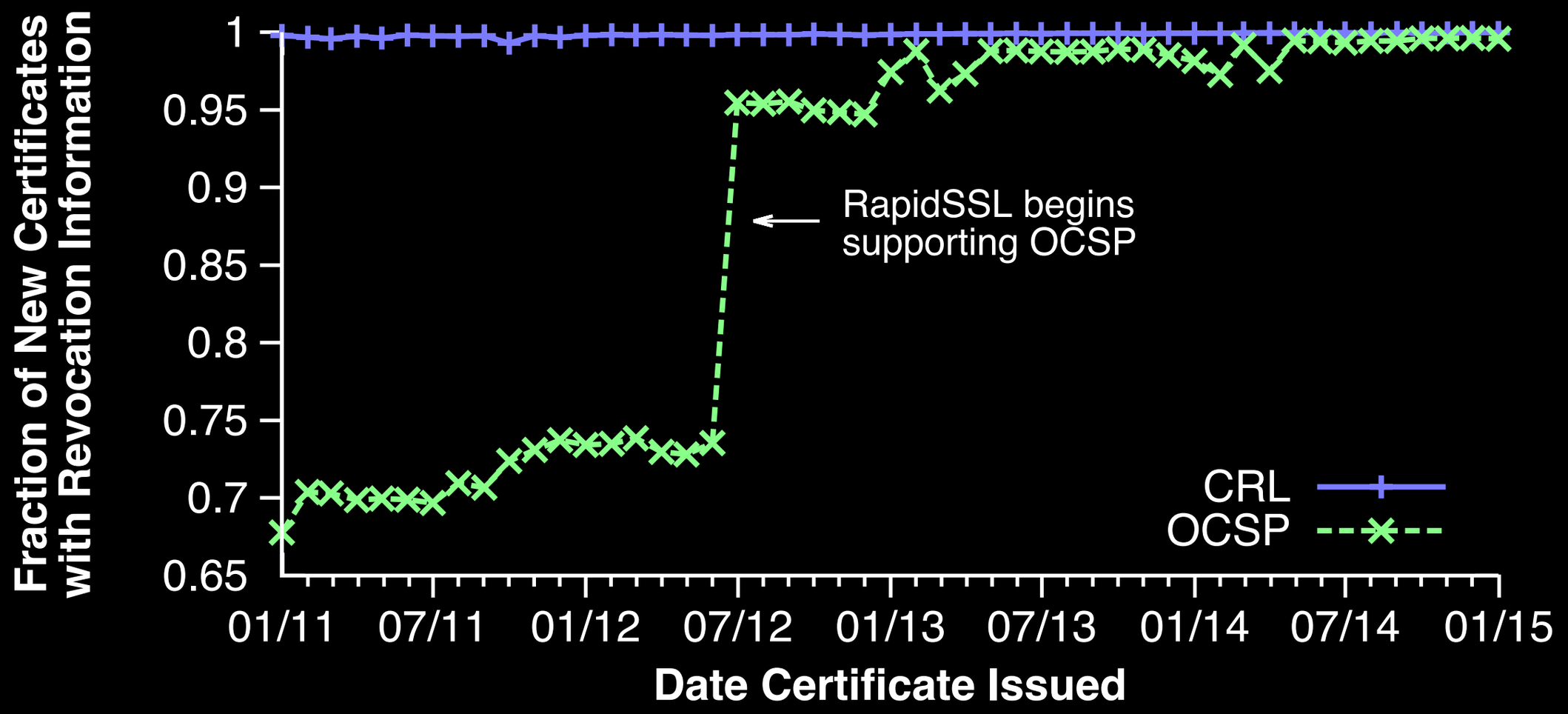
CRLs, OCSP, and OCSP Stapling



OCSP prevalence

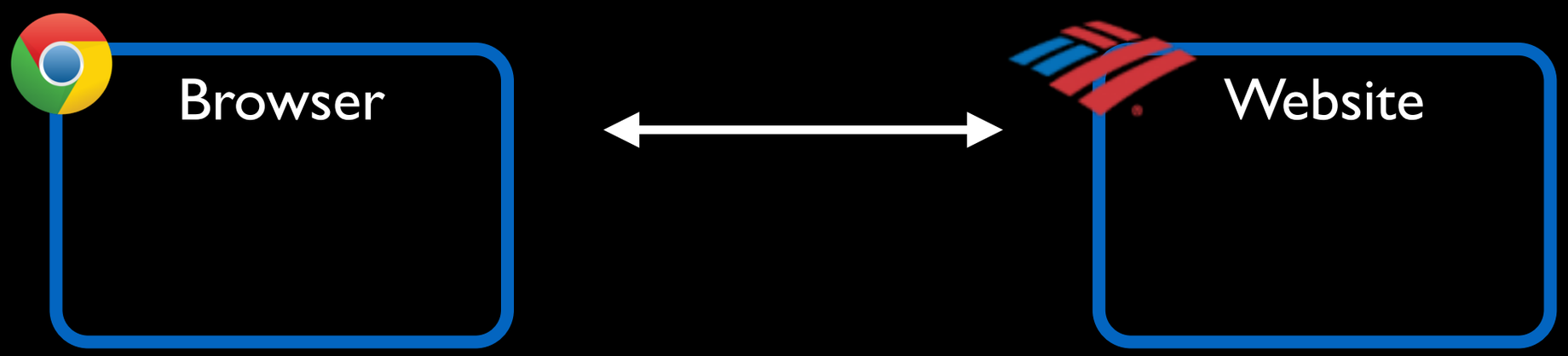


OCSP prevalence

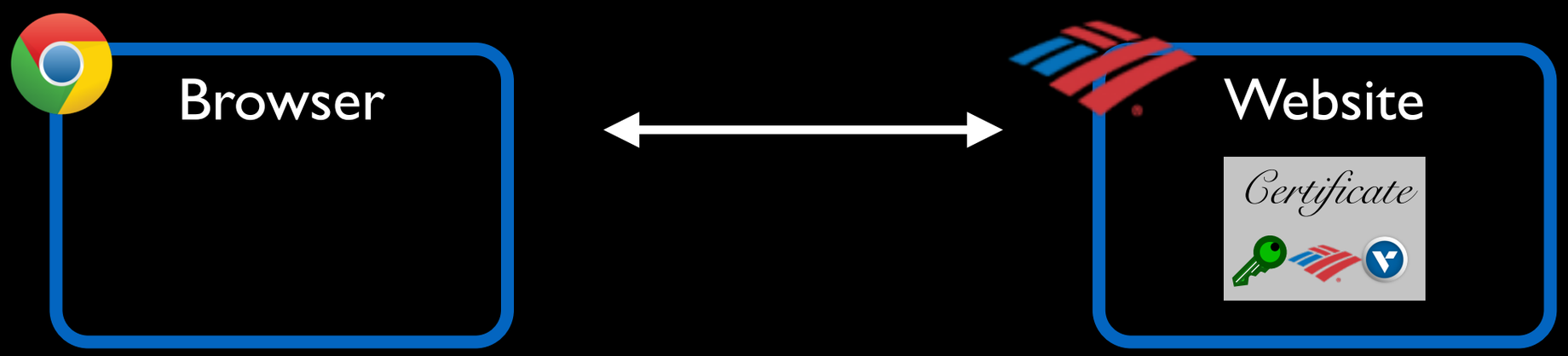


OCSP now universally supported

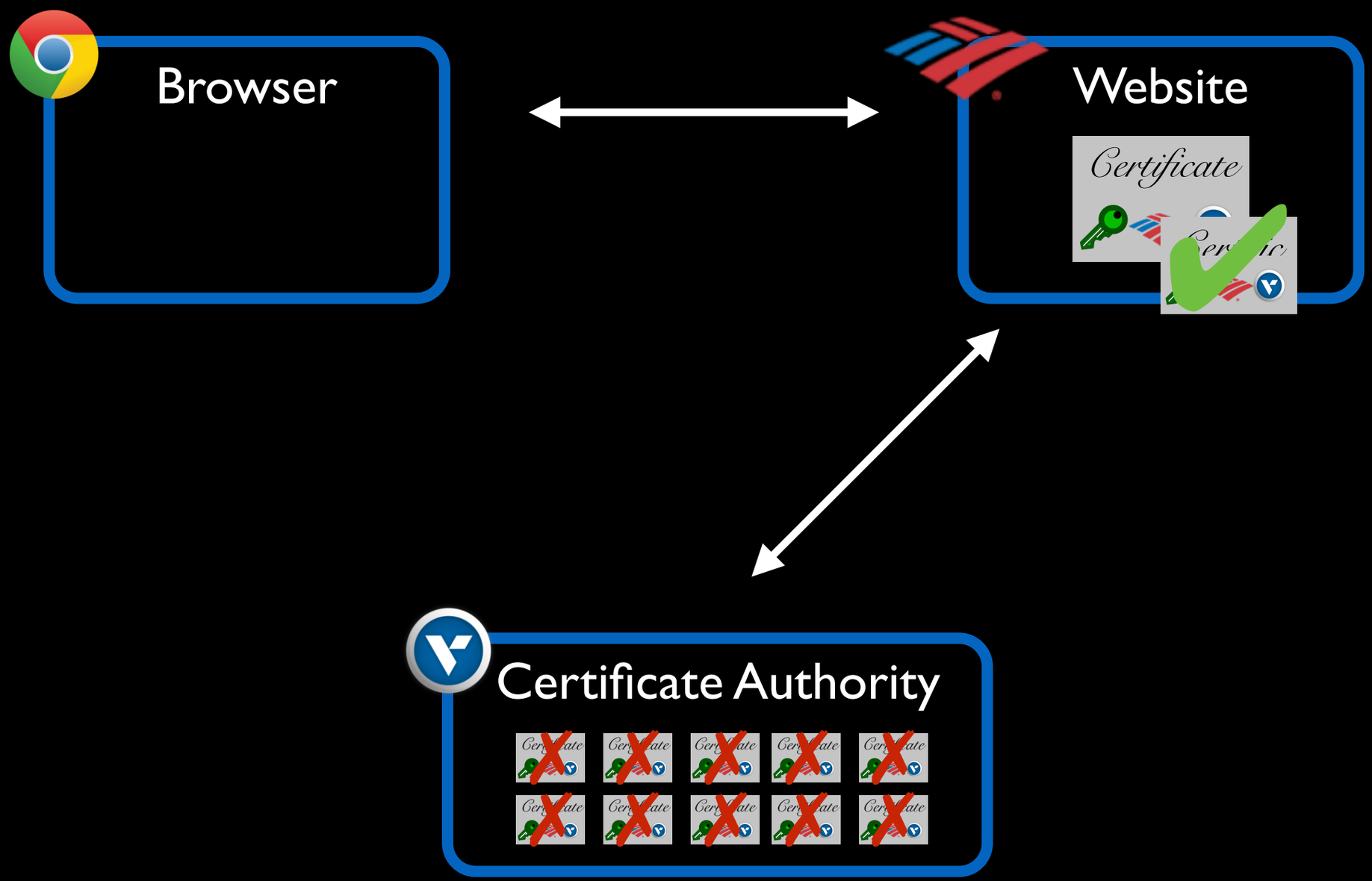
CRLs, OCSP, and OCSP Stapling



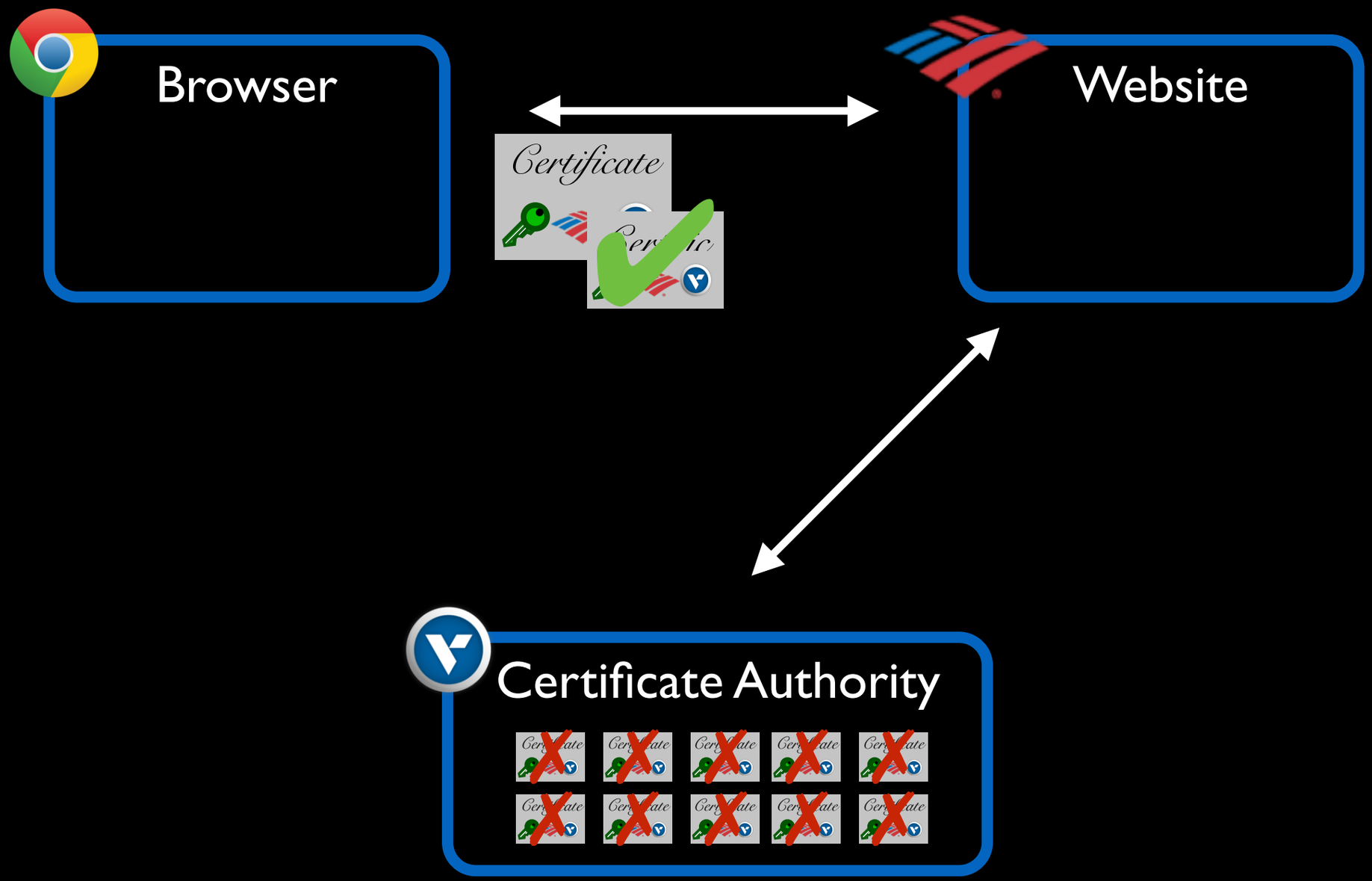
CRLs, OCSP, and OCSP Stapling



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?

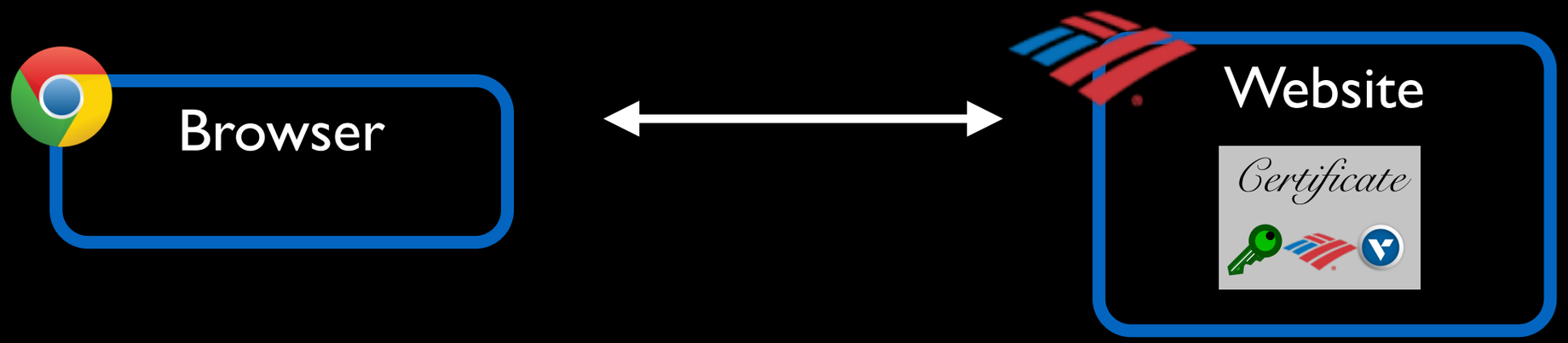
Outline

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

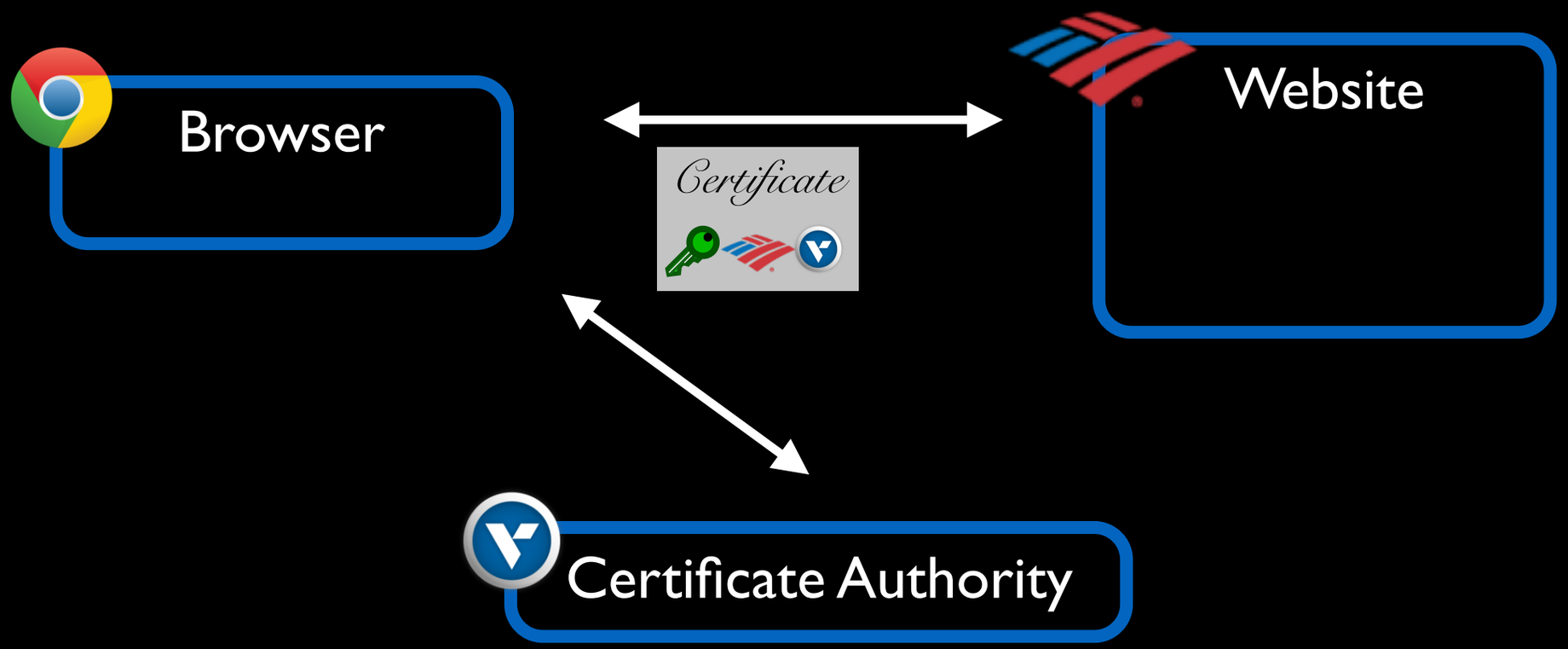
Certificate authorities behavior
e.g., high cost in distributing revocation info

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

What's the concern of browsers?



What's the concern of browsers?



On the web, latency is king

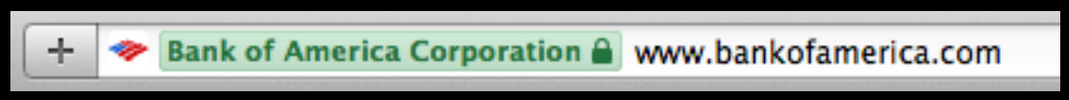
Browsers face tension between security and speed
Must contact CA to ensure cert not revoked

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 revocations?

Supports CRLs

Desktop: 

Mobile: 

Supports OCSP

Desktop: 

Mobile: 

Supports OCSP Stapling

Desktop: 

Mobile: 

Do browsers check revocations?

Supports CRLs

Desktop: 

EV only

Mobile: 

Supports OCSP

Desktop: 

Mobile: 

Supports OCSP Stapling

Desktop: 

Mobile: 

Do browsers check revocations?

Supports CRLs

Desktop: 
EV only

Mobile: 

Supports OCSP

Desktop: 
EV only

Mobile: 

Supports OCSP Stapling

Desktop: 

Mobile: 

Do browsers check revocations?

Supports CRLs

Desktop: 

EV only

Mobile: 

Supports OCSP

Desktop: 

EV only

Mobile: 

Supports OCSP Stapling

Desktop: 

Mobile: 

Do browsers check intermediates?

Check intermediate

Desktop: 

Mobile: 

Revocation unavailable

Desktop: 

Mobile: 

Do browsers check intermediates?

Check intermediate

Desktop: 

Mobile: 

Revocation unavailable

Desktop: 

Mobile: 

Do browsers check intermediates?

Check intermediate

Desktop: 

Mobile: 

Revocation unavailable

Desktop: 

Mobile: 

Do browsers check intermediates?

Check intermediate

Desktop: 

Mobile: 

Revocation unavailable

Desktop: 

Mobile: 

No browser correctly checks all 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

CRLSet

Chrome pushes out list of select revocations, called CRLSet

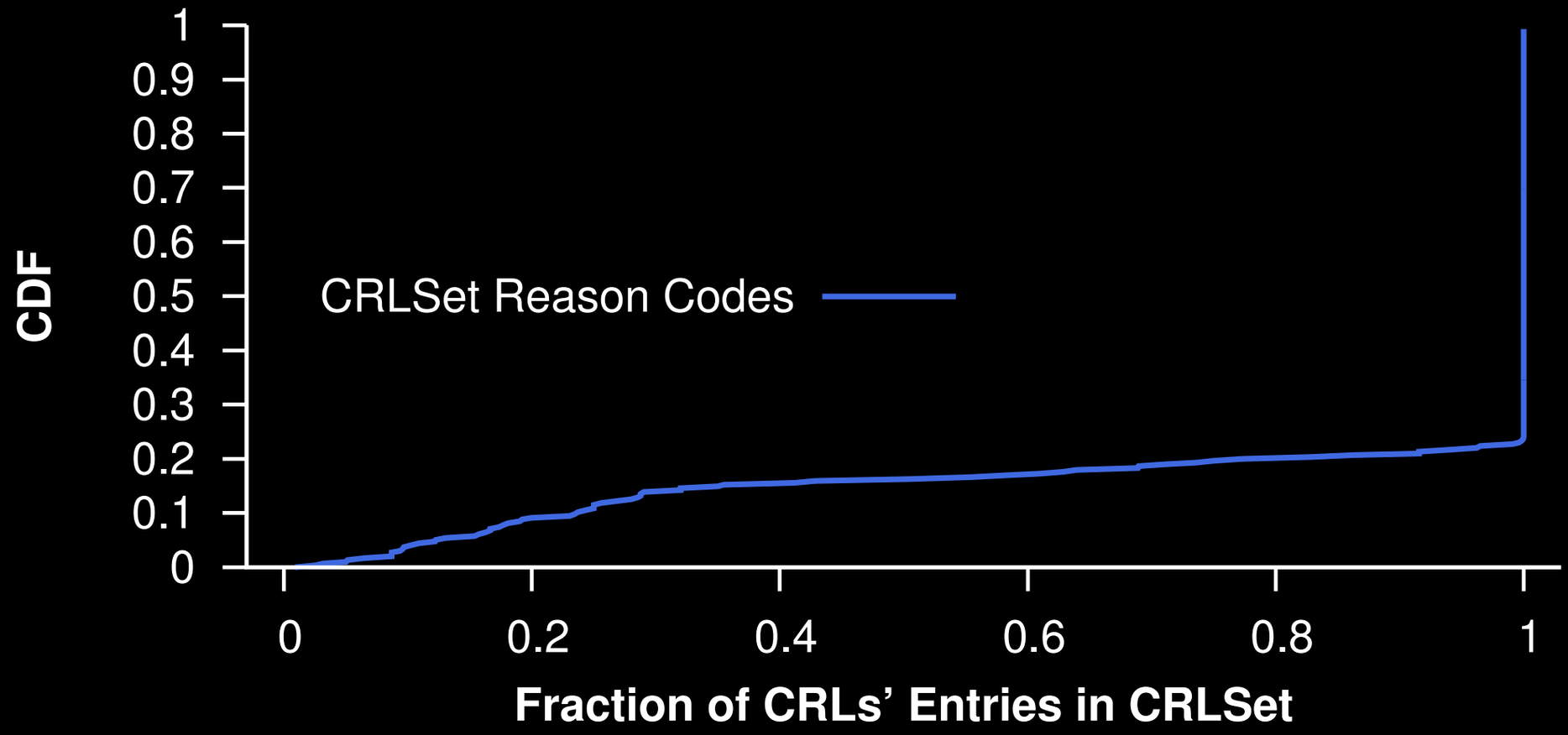
Chromium developers only state:

1. The full list [of covered CRLs] isn't public
2. CRLs on the list are fetched infrequently
3. Entries in the CRL are filtered by reason code.
4. Size limited to 250 KB

CRLSet coverage

Only 0.35% of all revocations appear in CRLSet

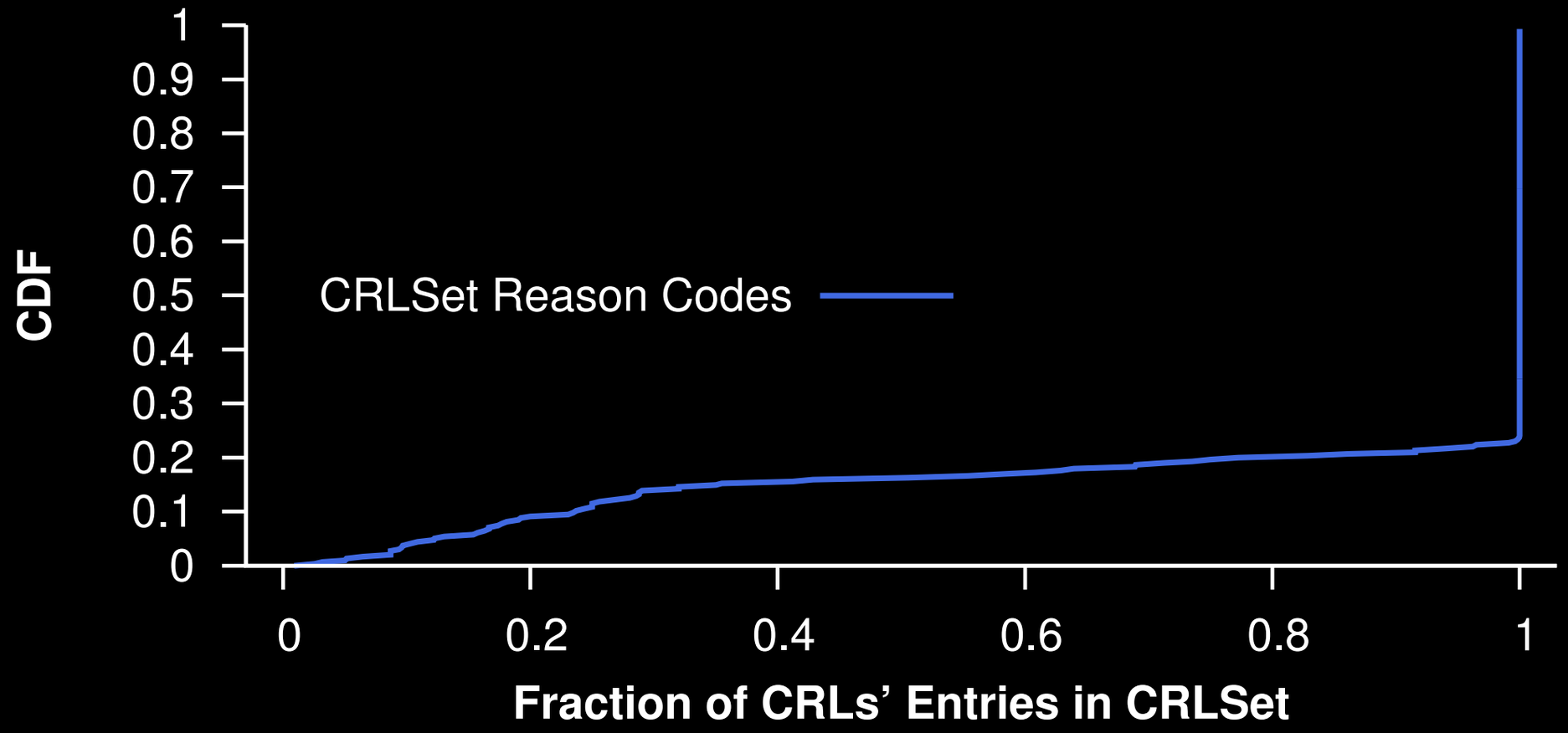
Only 295 (10.5%) CRLs have *any* revocations covered



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

More results in the paper

- Analysis of EV certificate revocation
- Revoked but alive certificates
- 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