Is the Web Ready for OCSP Must-Staple?

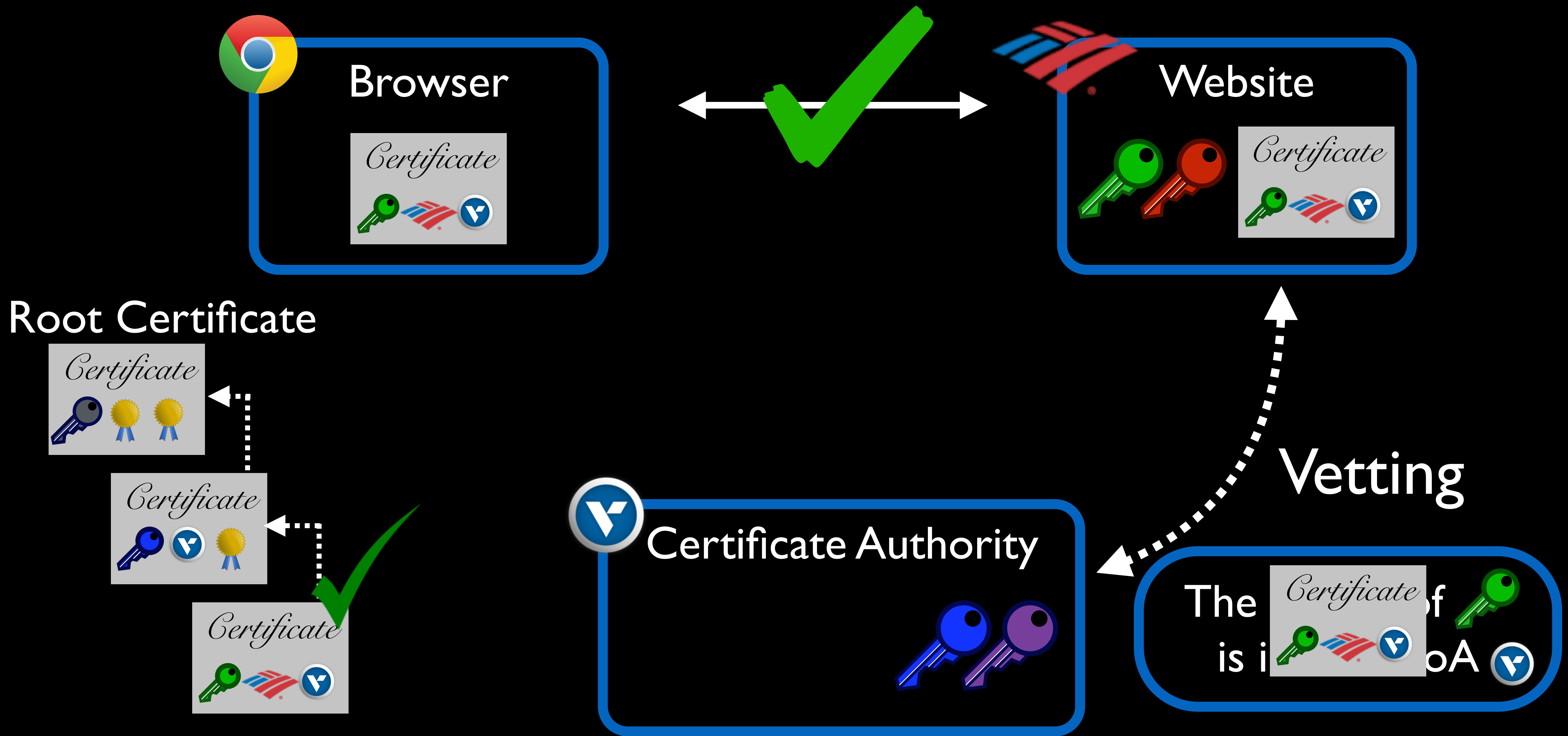
Taejoong (Tijay) Chung*, Jay Lok, Bala Chandrasekaran
David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove,
John Rula, Nick Sullivan, Christo Wilson

*This work was done while the author was a postdoctoral researcher at Northeastern University

Is the Web Ready for OCSP Must-Staple?

How HTTPS Works

How can users truly know with whom they are communicating?



Browser

Certificate

Website

Certificate

Root Certificate

Certificate

Certificate

Certificate

Vetting

Certificate Authority

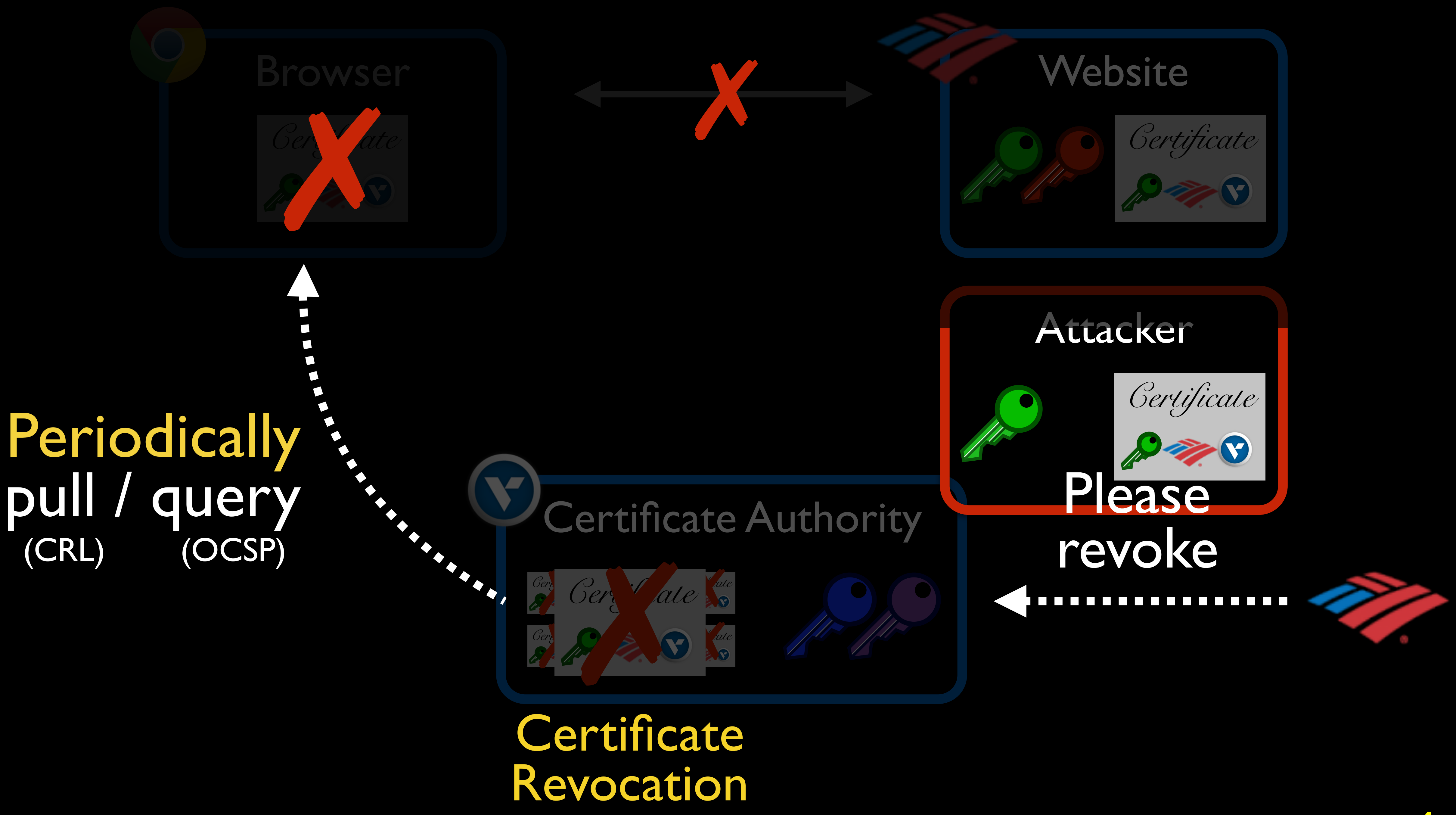
The Certificate f

is i oA

Certificate

Certificate revocation

What happens when a certificate is no longer valid?



Browser

Website

Attacker

Please revoke

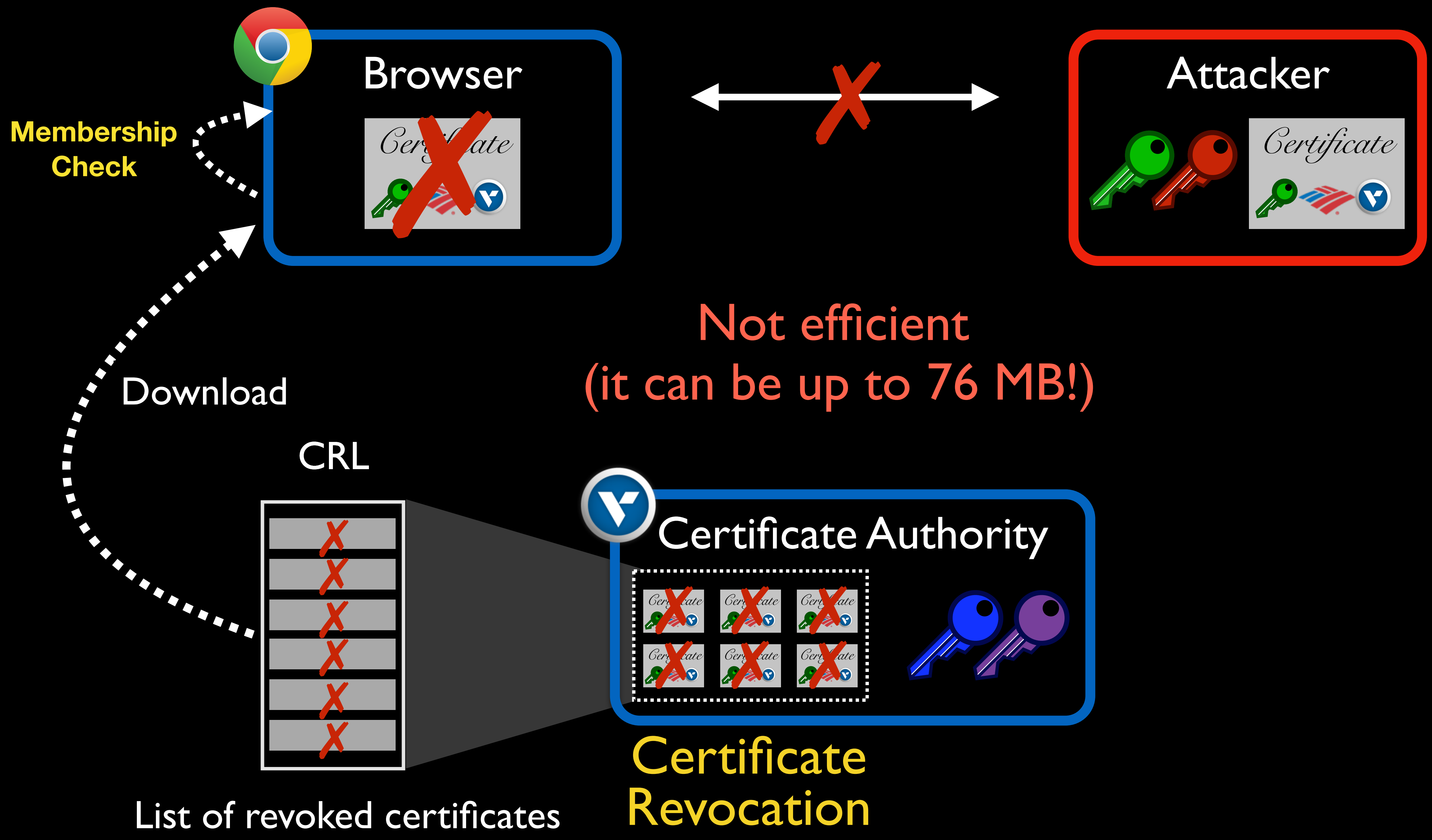
Periodically pull / query

(CRL) (OCSP)

Certificate Authority

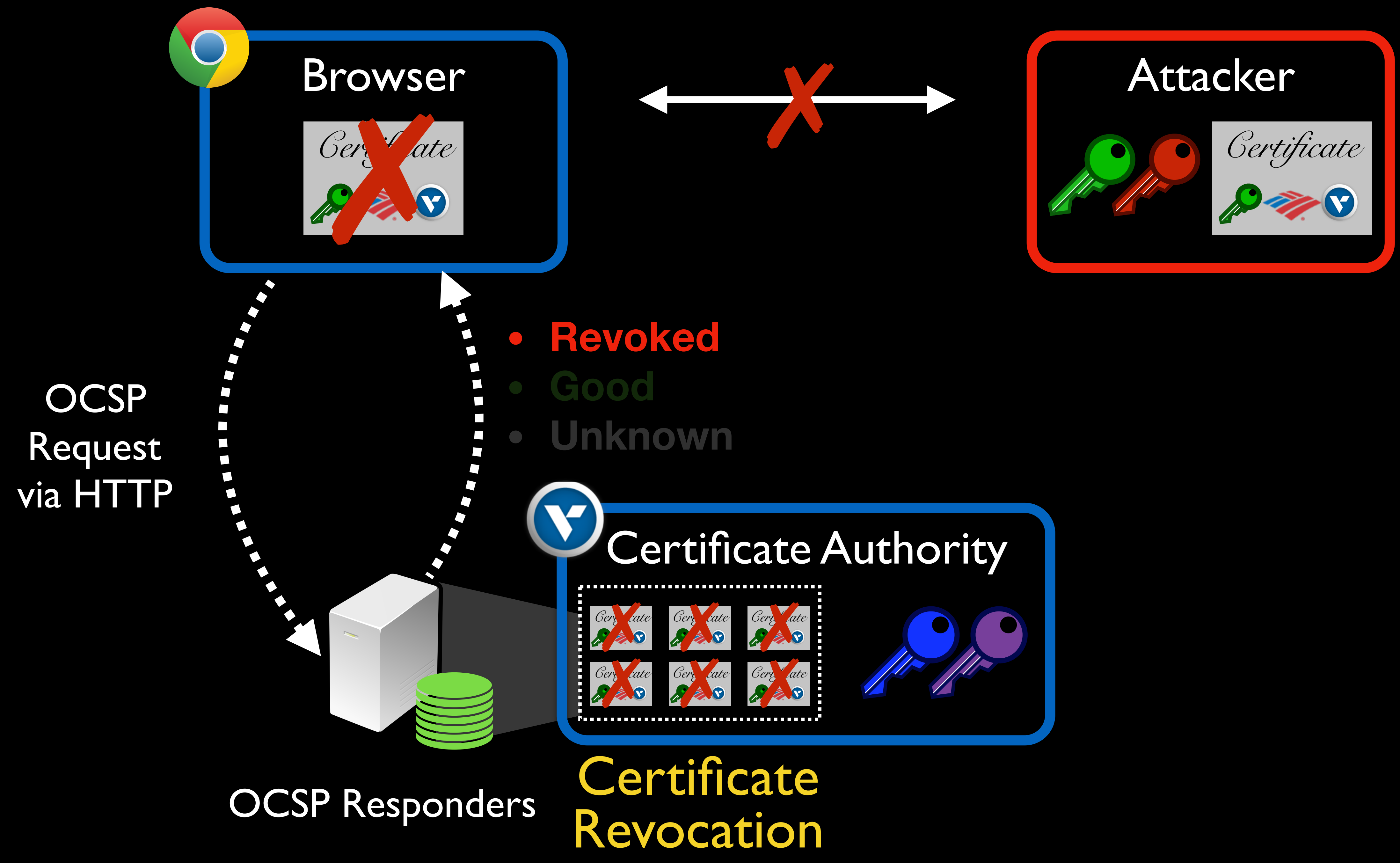
Certificate Revocation

Revocation Check (1)
Certificate Revocation List



Not efficient
(it can be up to 76 MB!)

Revocation Check (2)
Online Certificate Status Protocol



Browser

Attacker

- Revoked
- Good
- Unknown

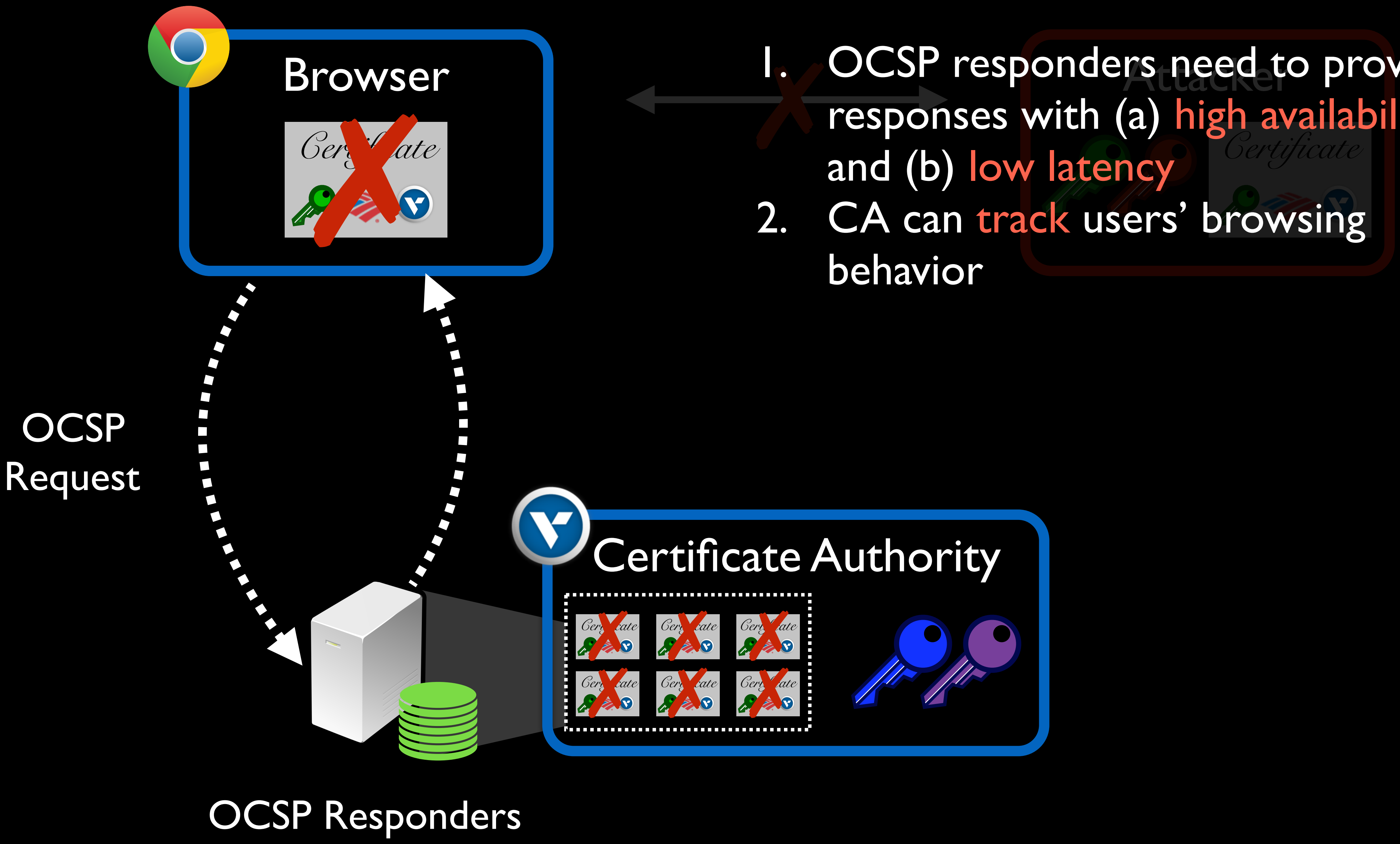
OCSP Request via HTTP

Certificate Authority

OCSP Responders

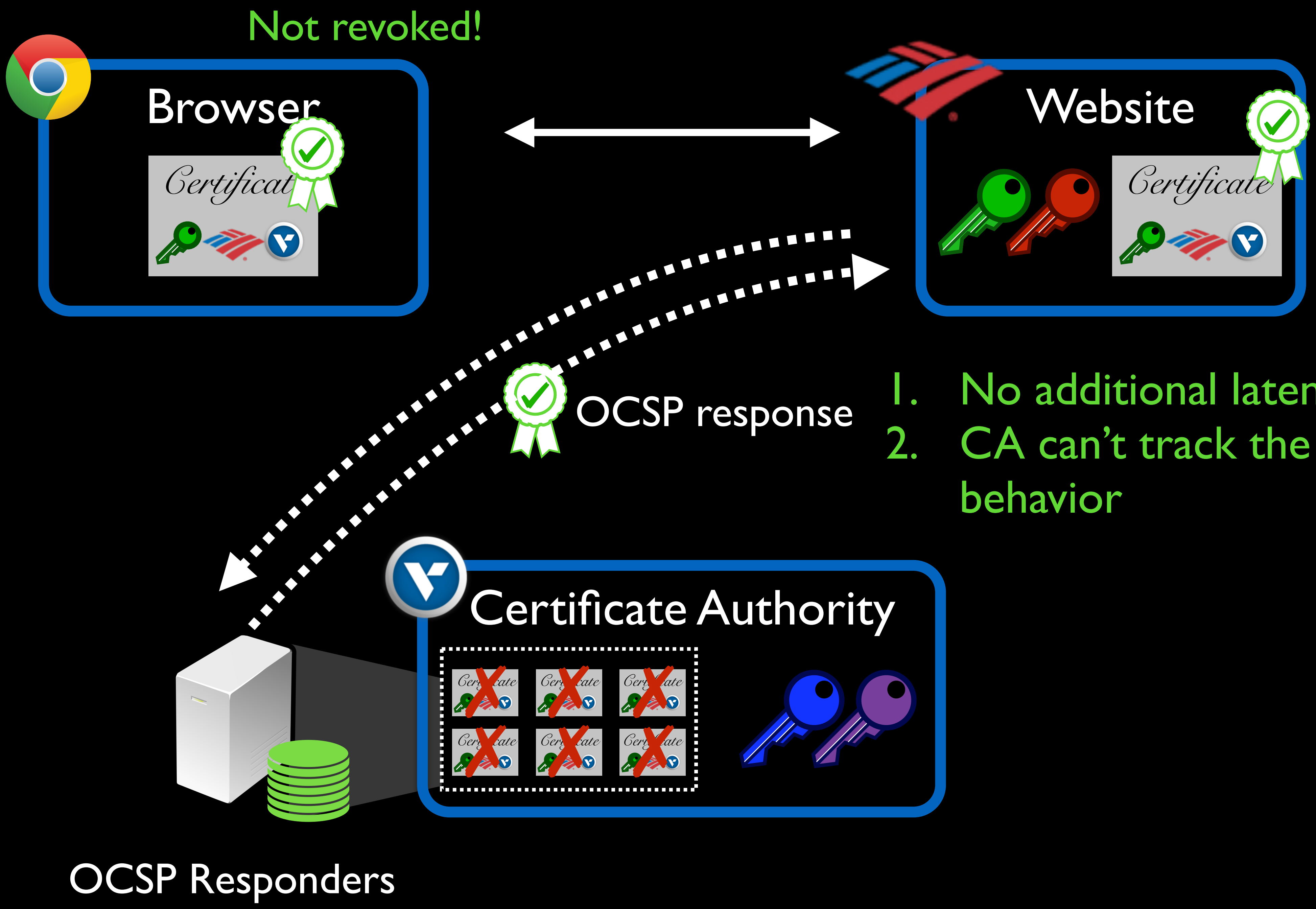
Certificate Revocation

Challenges of
Online Certificate Status Protocol



1. OCSP responders need to provide responses with (a) high availability and (b) low latency
2. CA can track users' browsing behavior

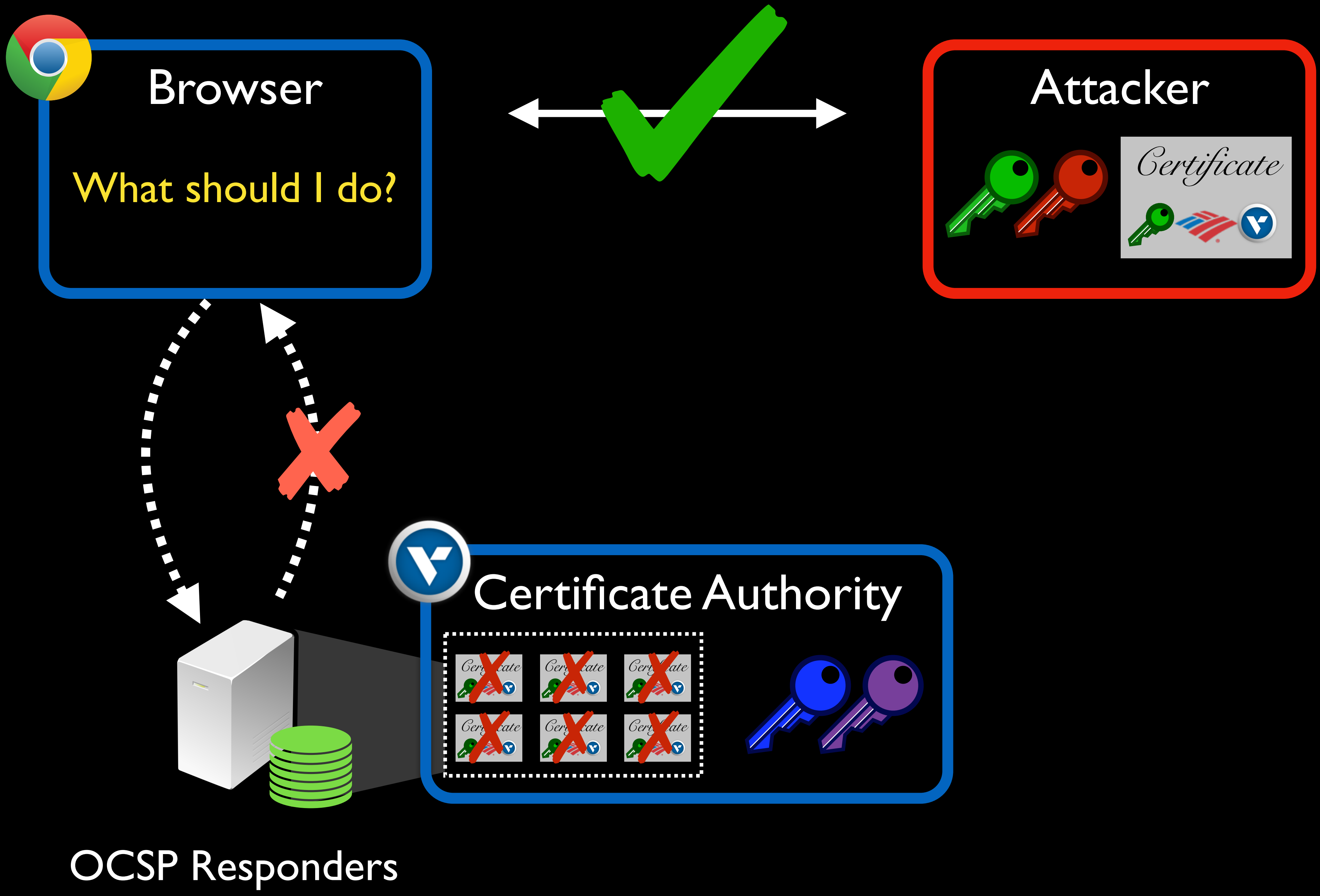
OCSP Stapling



1. No additional latency
2. CA can't track the browsing behavior

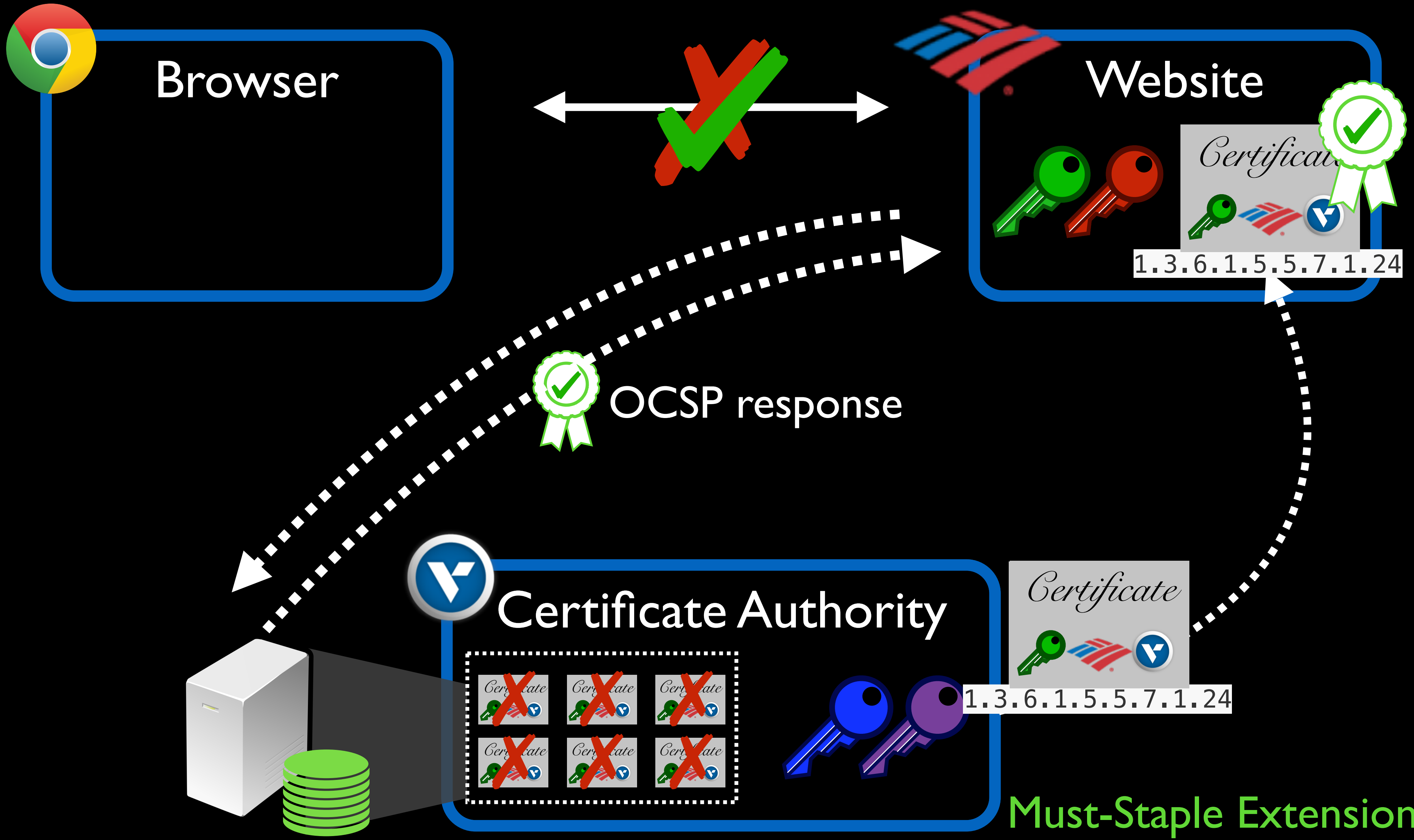
Challenges still remain:
Soft failure

Most clients will accept a certificate
even if they are unable to obtain revocation information



OCSP Must-Staple

- ✓ No additional latency
- ✓ No privacy issues
- ✓ No soft failure



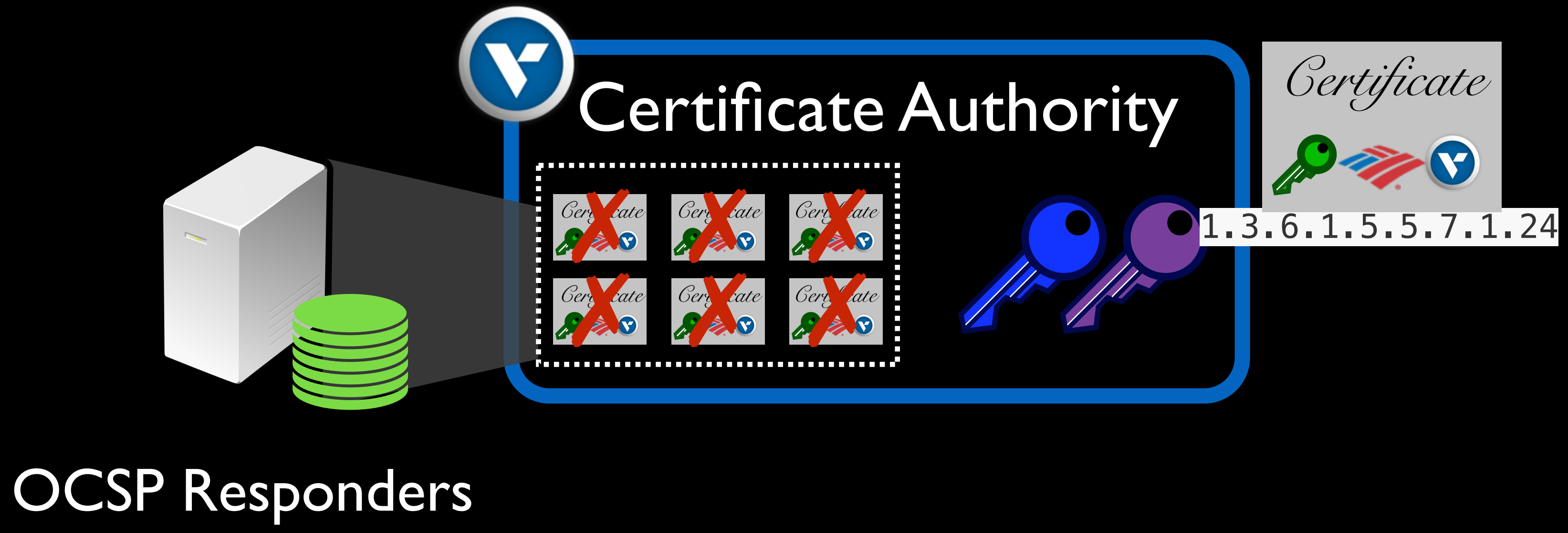
OCSP Responders

Must-Staple Extension:
The server will provide a valid OCSP response

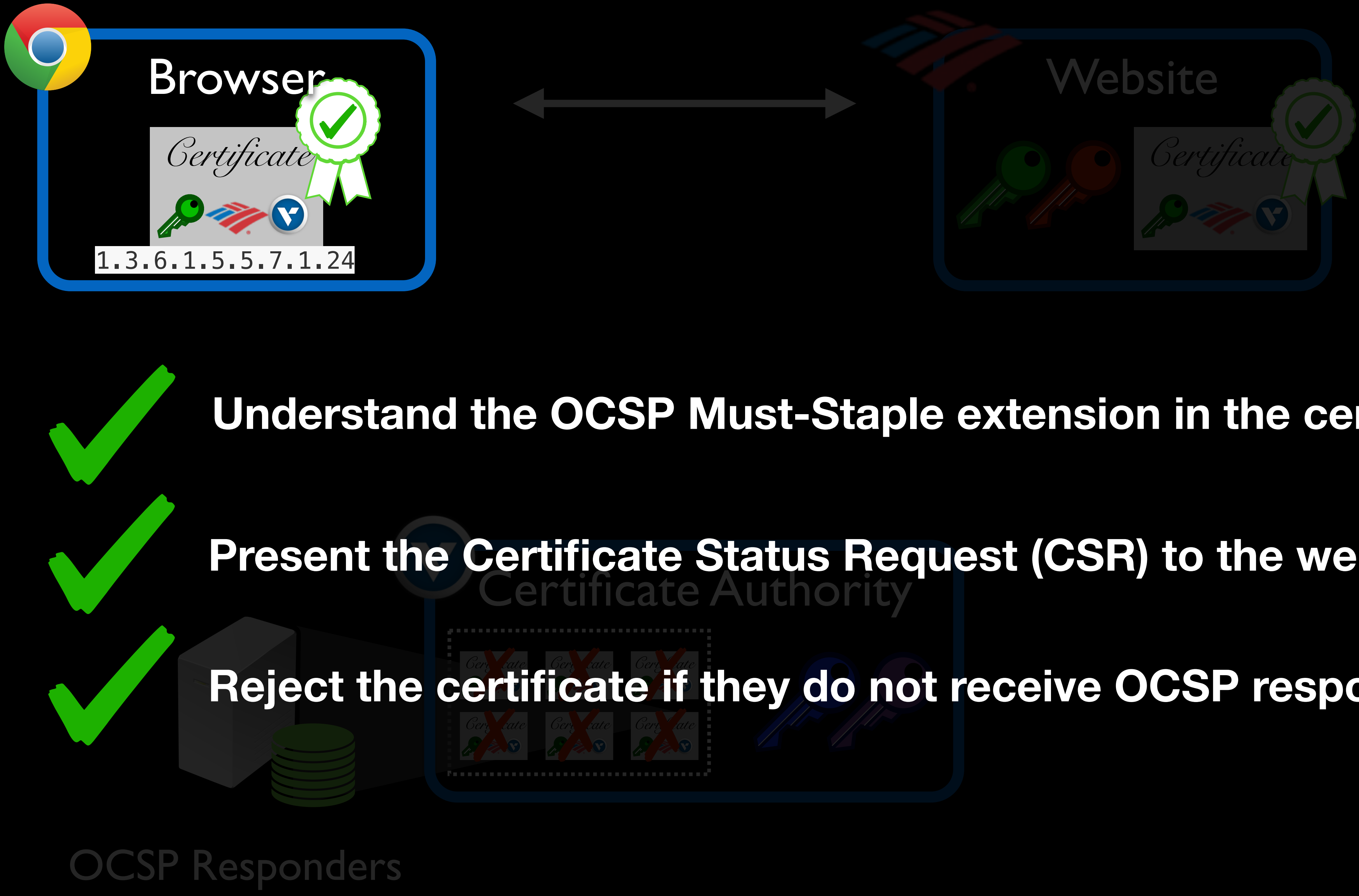
To support OCSP Must Staple
(1) CA

✓ **Include the OCSP Must-Staple extension into certificates**

✓ **Run reliable/error-free OCSP responders**

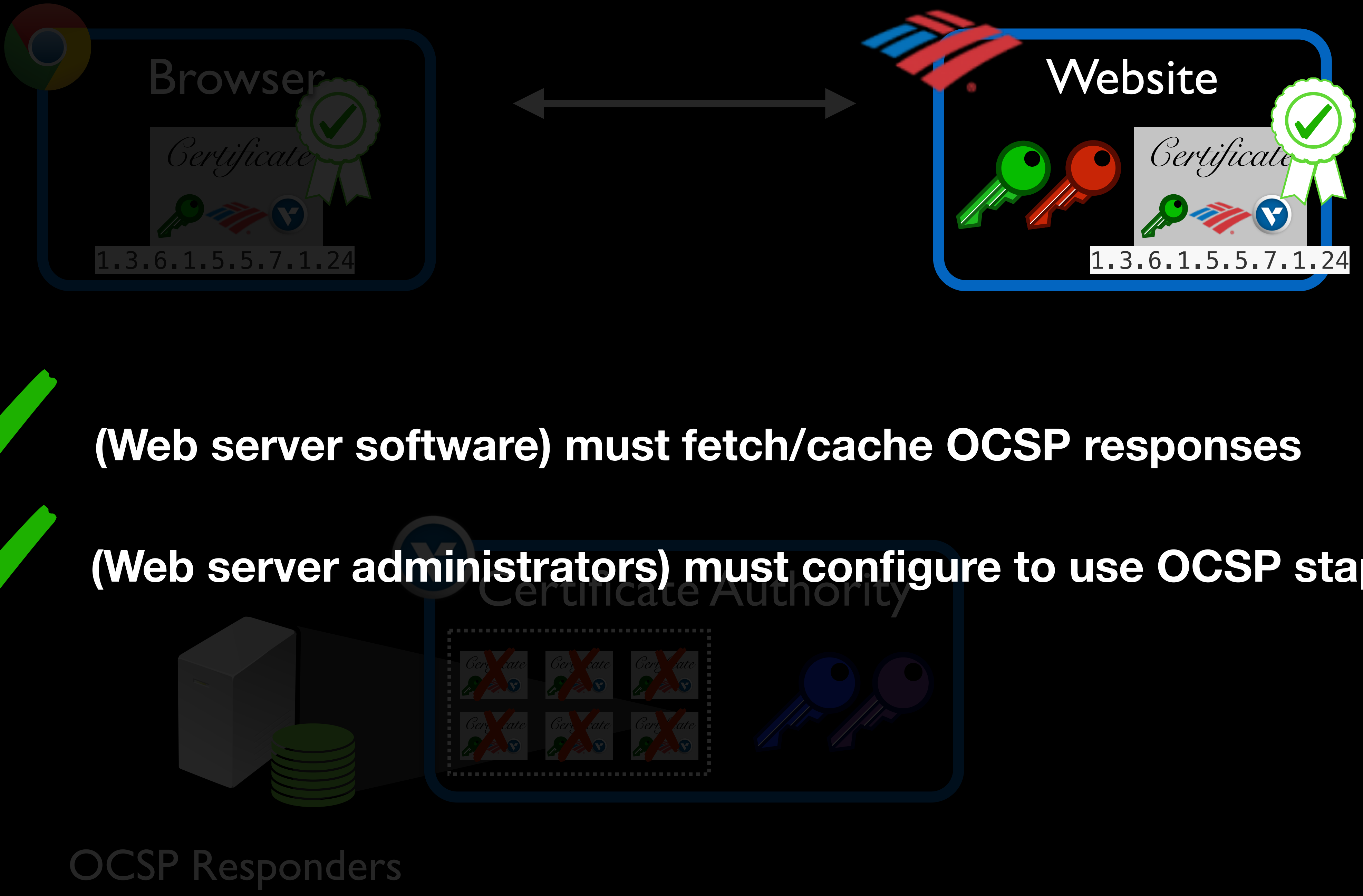


To support OCSP Must Staple
(2) Clients



- ✓ **Understand the OCSP Must-Staple extension in the certificate**
- ✓ **Present the Certificate Status Request (CSR) to the web servers**
- ✓ **Reject the certificate if they do not receive OCSP responses**

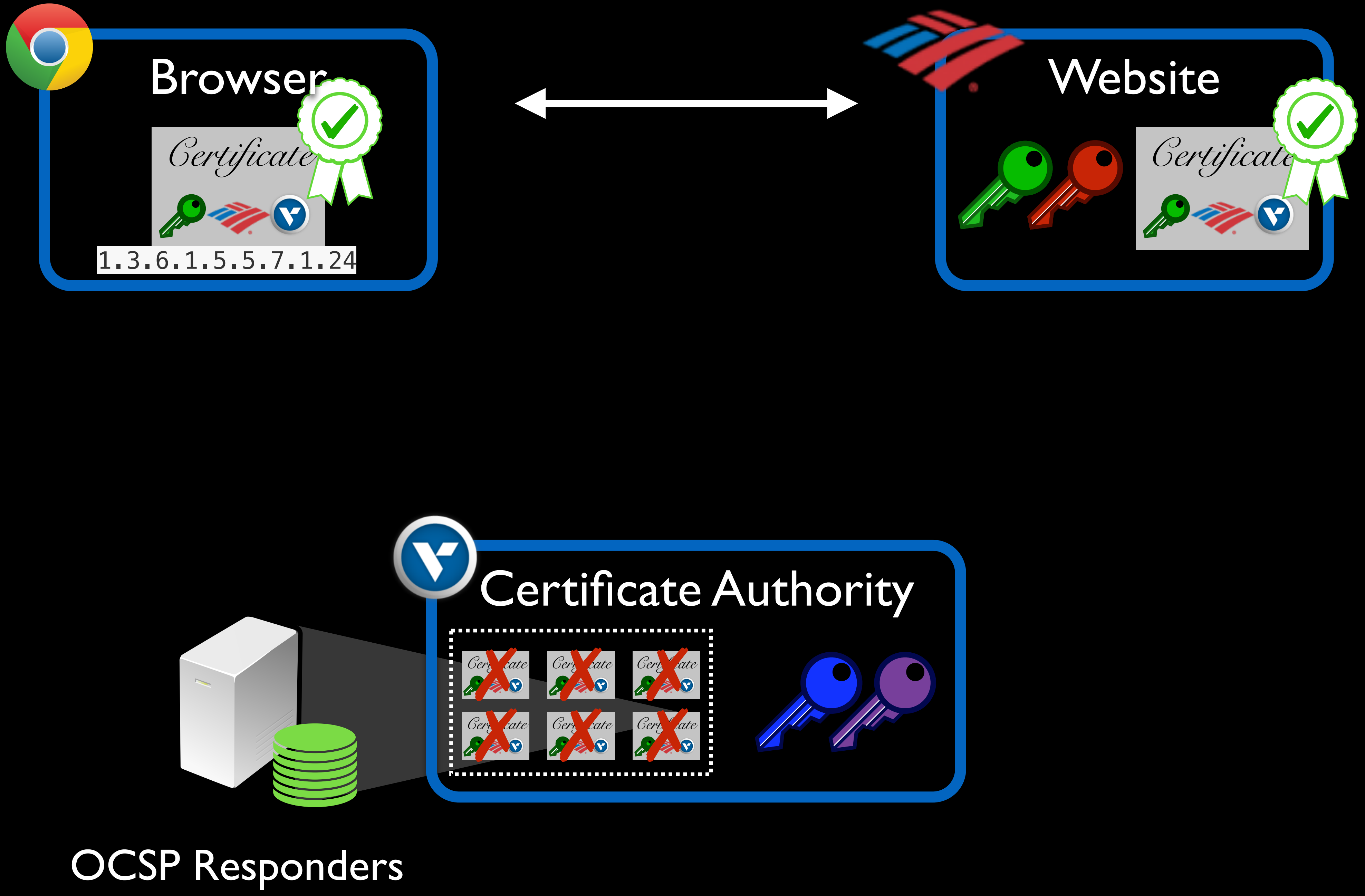
To support OCSP Must Staple
(3) Web servers



✓ **(Web server software) must fetch/cache OCSP responses**

✓ **(Web server administrators) must configure to use OCSP stapling**

To support OCSP Must Staple



Is the Web Ready for OCSP Must-Staple?

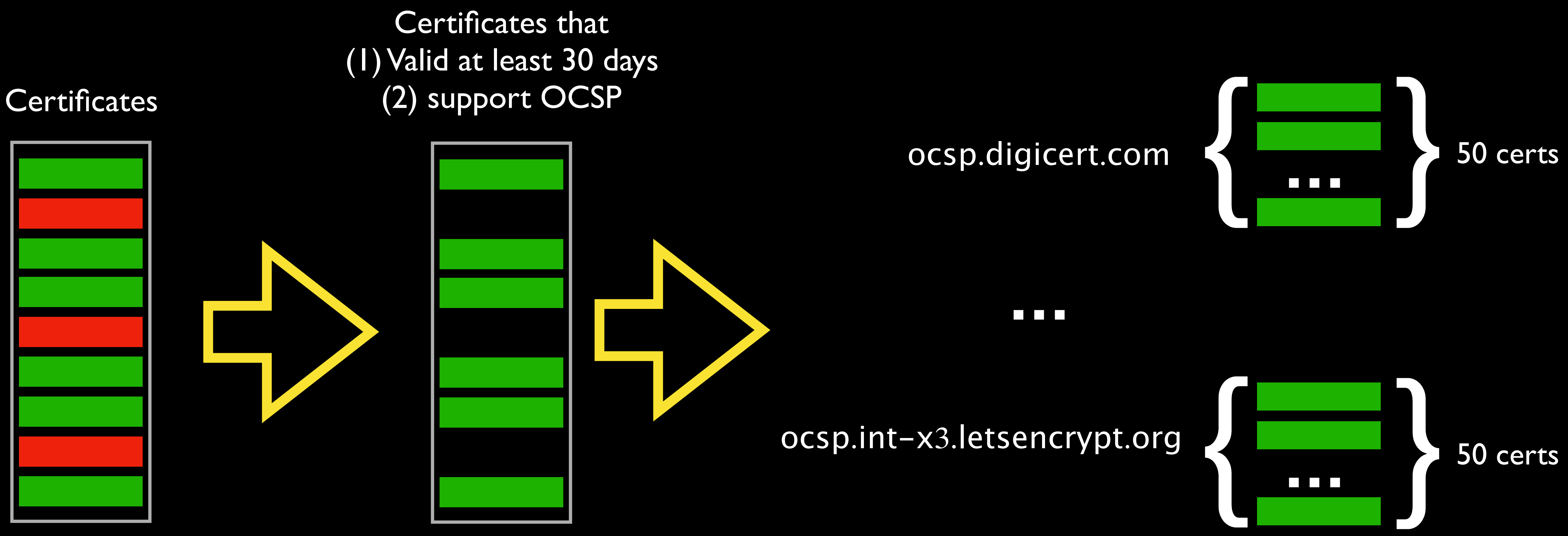
Certificate Authority
(OCSP Responder)

- ✓ Availability
- ✓ Validity
- ✓ Consistency with CRL

Website

Browser

Measuring OCSP Responders



Certificates

Certificates that
(1) Valid at least 30 days
(2) support OCSP

ocsp.digicert.com

50 certs

...

ocsp.int-x3.letsencrypt.org

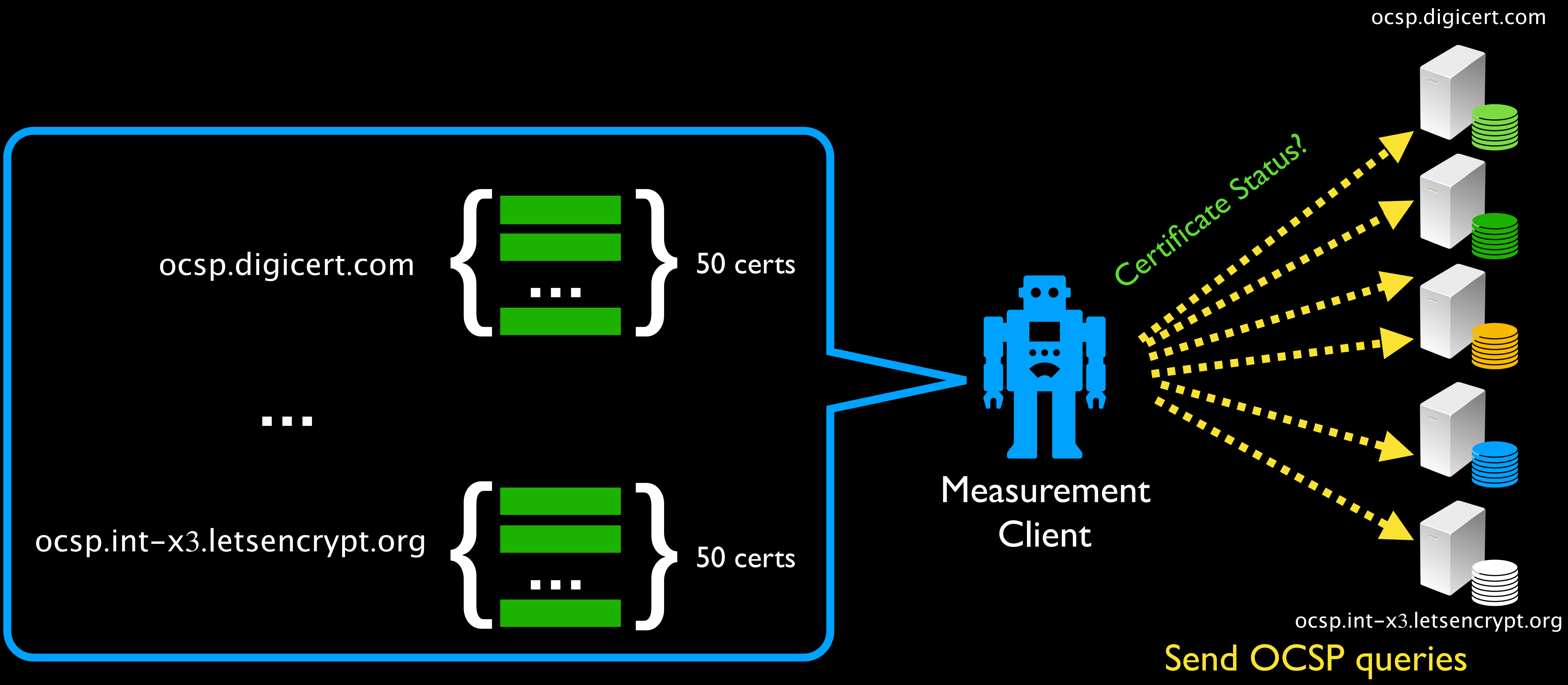
50 certs

112 M certificates

77 M certificates

536 OCSP responders
with 14,634 certificates

Measuring OCSP Responders



Send OCSP queries

Measurement

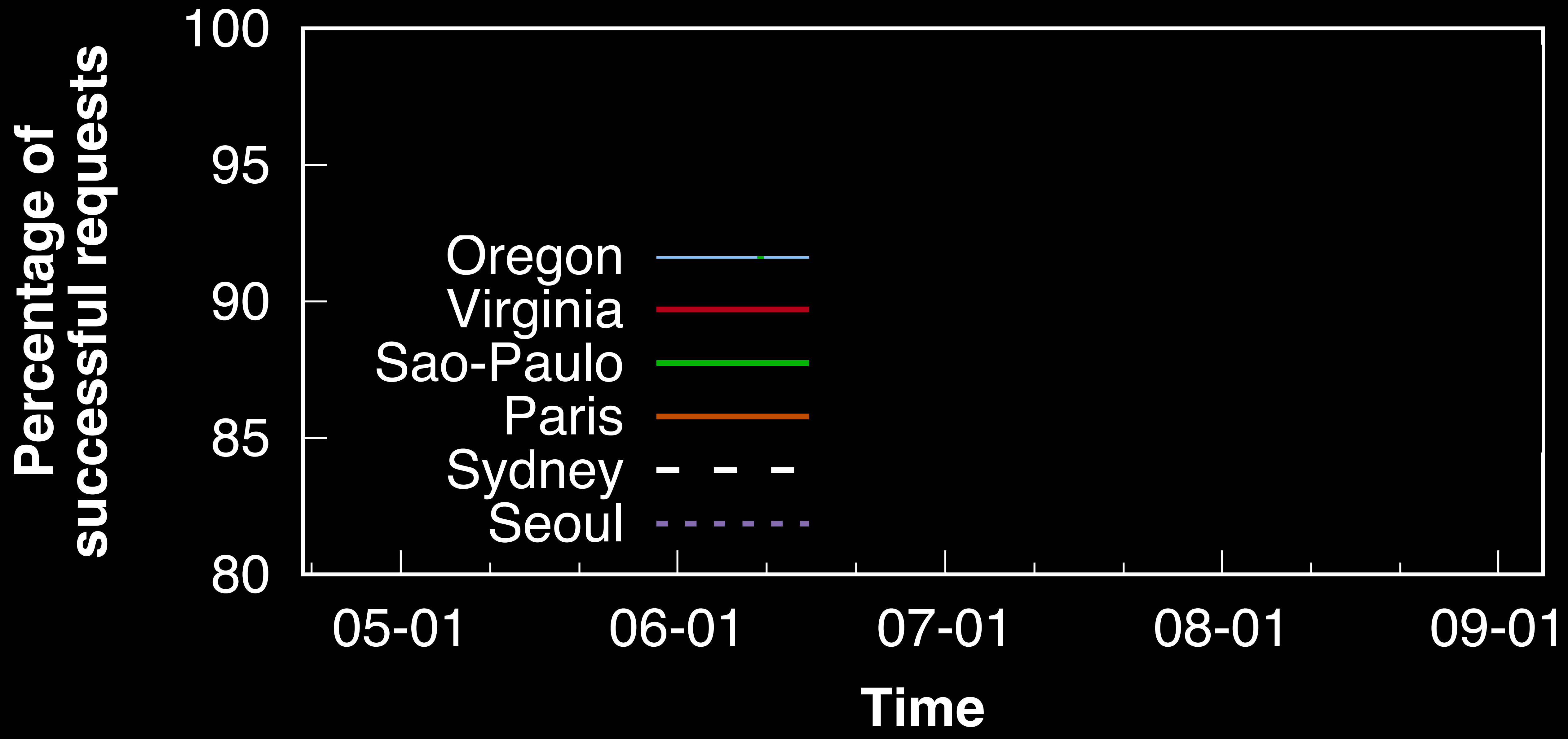
AWS

- Oregon (US West)
- Virginia (US East)
- São Paulo (Brazil)
- Paris (France)
- Sydney (Australia)
- Seoul (Korea)

Scan them every hour
April 25, 2018 ~ September 4, 2018

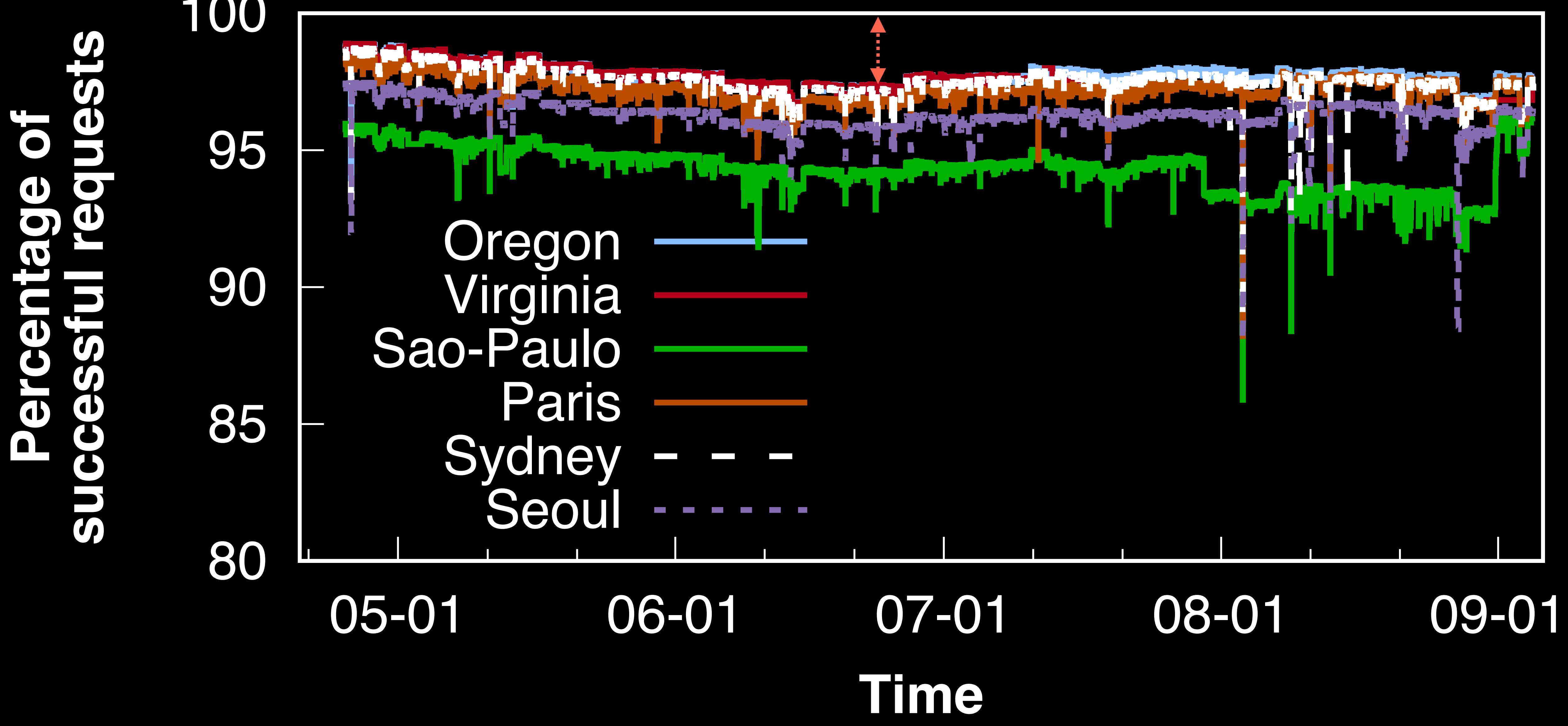
~ 46 M OCSP requests & responses

(1) Availability



(1) Availability Overview

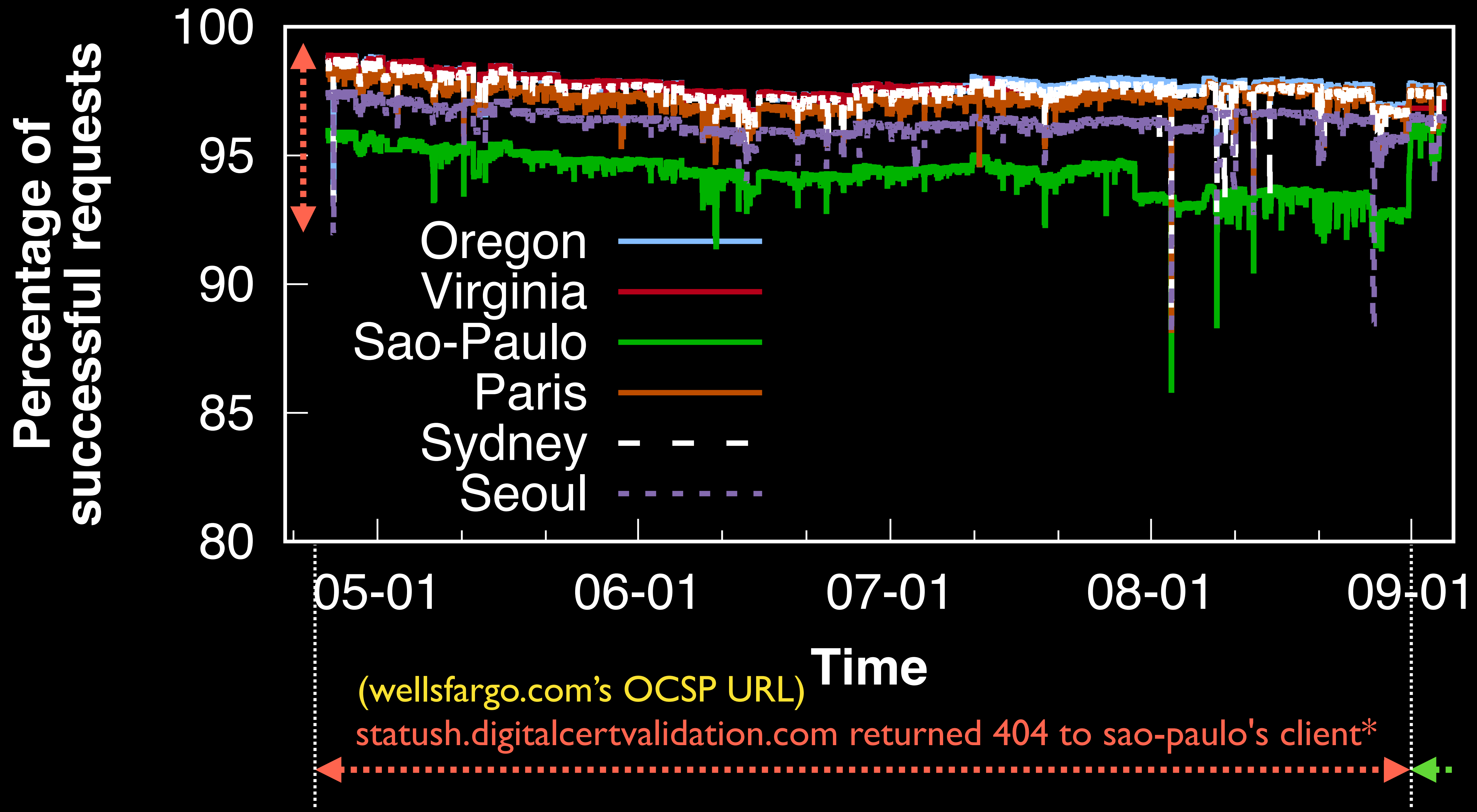
We're never able to receive successful responses from all OCSP responders



For 29 OCSP responders, there was at least one measurement client that was never able to make a successful request.

(16: DNS problem, 4: TCP connection errors, 8: HTTP problems, 1: HTTPS Error)

(1) Availability: Geographical Differences



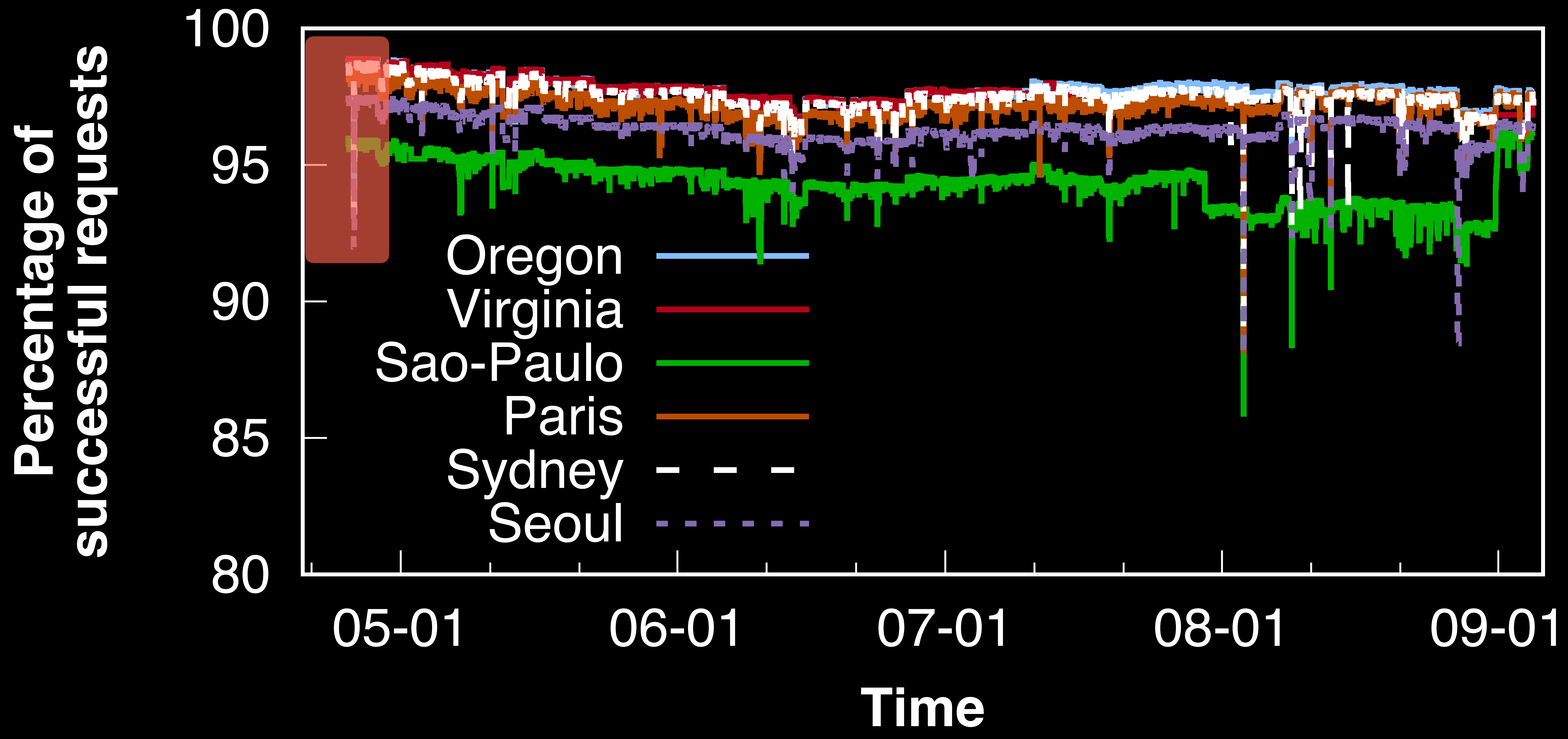
(wellsfargo.com's OCSP URL)

statush.digitalcertvalidation.com returned 404 to sao-paulo's client*

*After we contacted them on August 29th, the issue was fixed at 11pm August 31st.

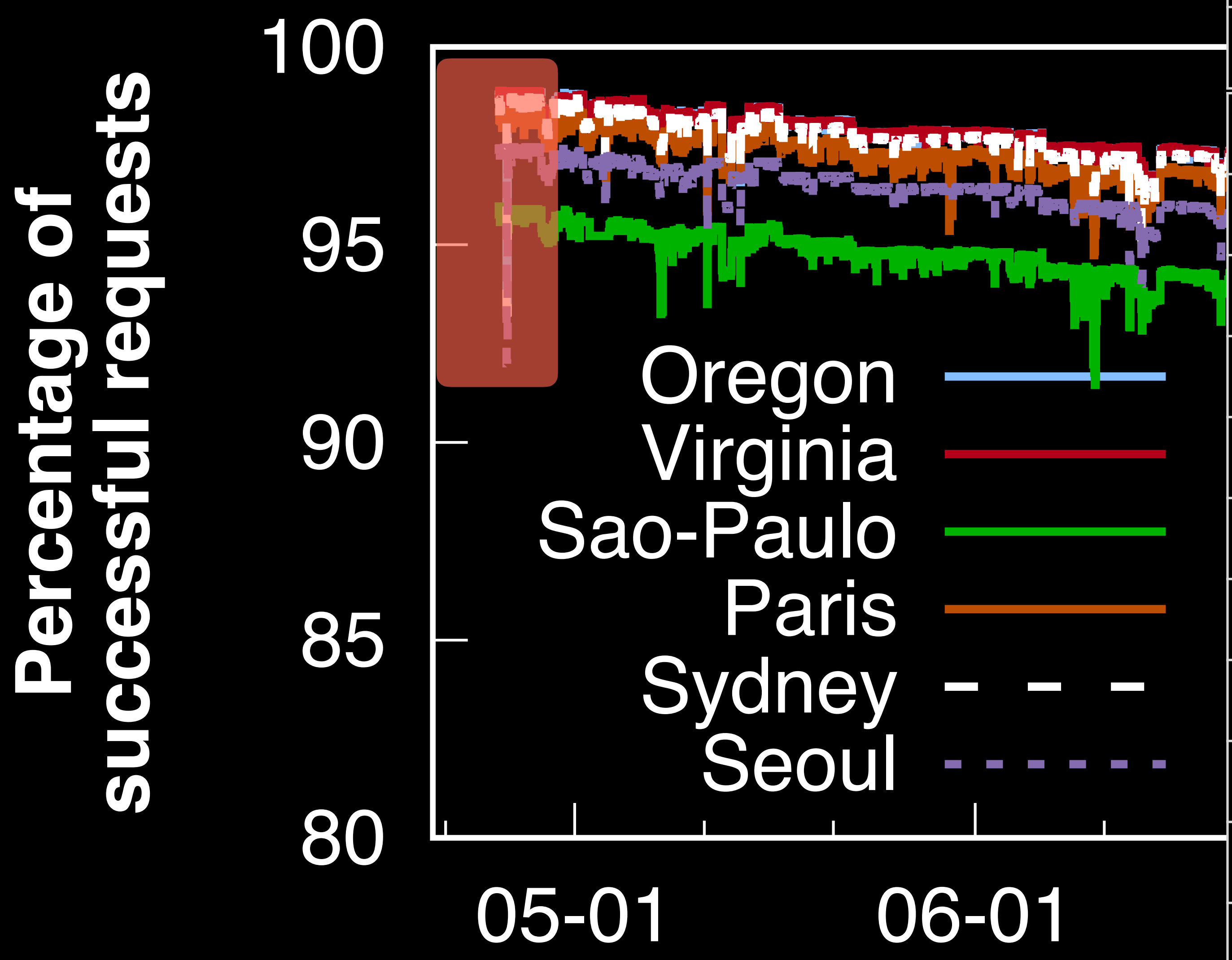
(1) Availability: Transient Failure

Seoul, Sydney, and Oregon (Asia Pacific)



(1) Availability:
Transient Failure (Case-Study)

Seoul, Sydney, and Oregon (Asia Pacific)



OCSP Server Name	DNS Records
ocsp.comodoca.com	
ocsp.comodoca4.com	
ocsp.gandi.net	CNAME: ocsp.comodoca.com
ocsp.globessl.com	CNAME: ocsp.comodoca.com
ocsp.incommon-ecc.org	CNAME: ocsp.comodoca.com
ocsp.incommon-igtf.org	NS: ns0.comododns.com.
ocsp.incommon-rsa.org	NS: ns0.comododns.com.
OCSP.intel.com	CNAME: ocsp.comodoca.com
ocsp.marketware.eu	CNAME: ocsp.comodoca.com
ocsp.netsolssl.com	CNAME: ocsp.comodoca.com
ocsp.register.com	CNAME: ocsp.comodoca.com
ocsp.securecore-ca.com	NS: ns0.comododns.com.
ocsp.sgssl.net.	NS: ns0.comododns.com.
ocsp.trustasiassl.com.	NS: ns0.comododns.com.
ocsp.trust-provider.com	CNAME: ocsp.comodoca.com
ocsp.usertrust.com	NS: ns0.comododns.com.

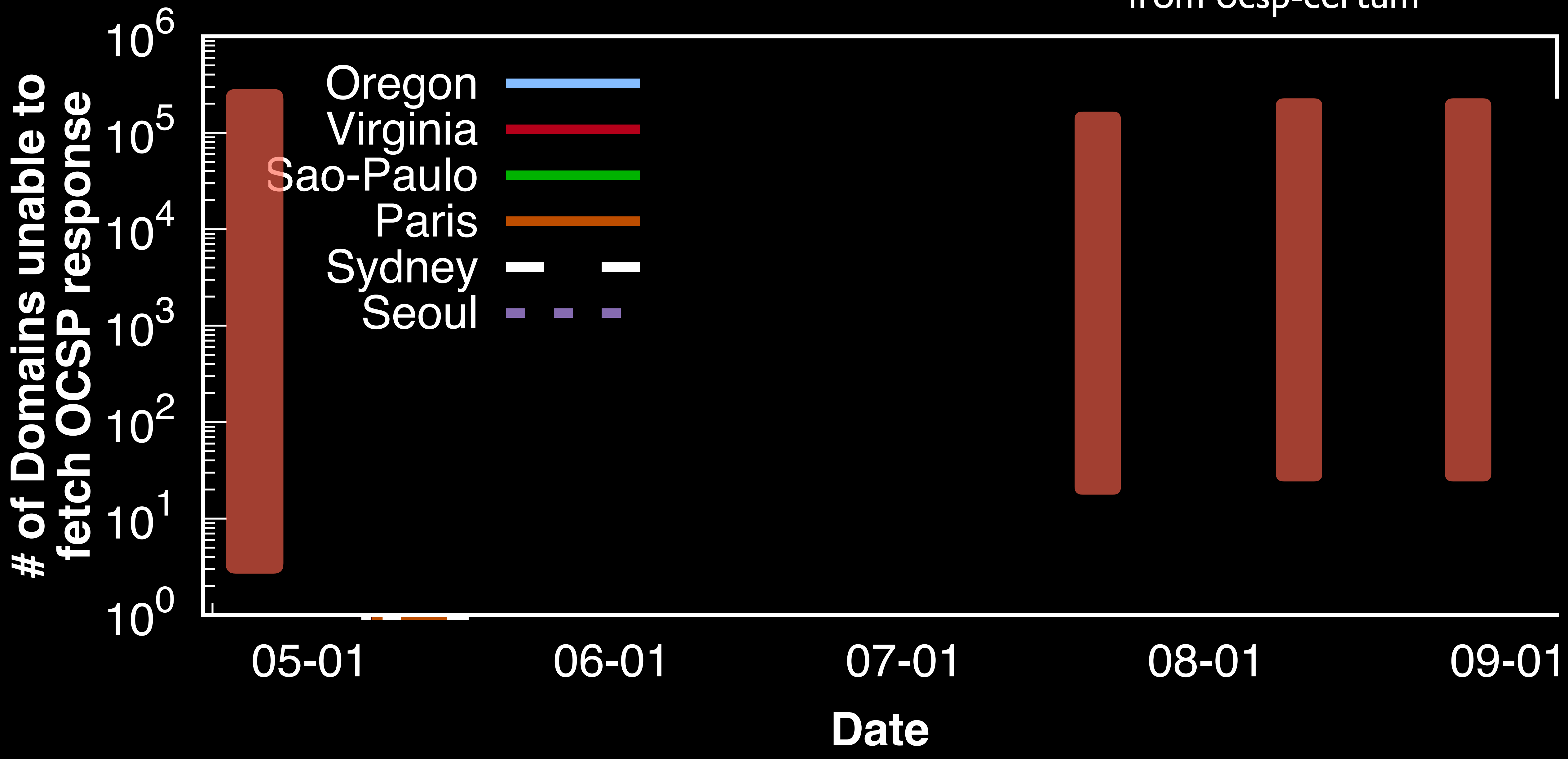
(1) Availability:
Impact on the Web

Comodo
down for 2 hours

43 servers from wosign
5 servers from startssl

16 servers
from ocsp-certum

9 servers
from digicert

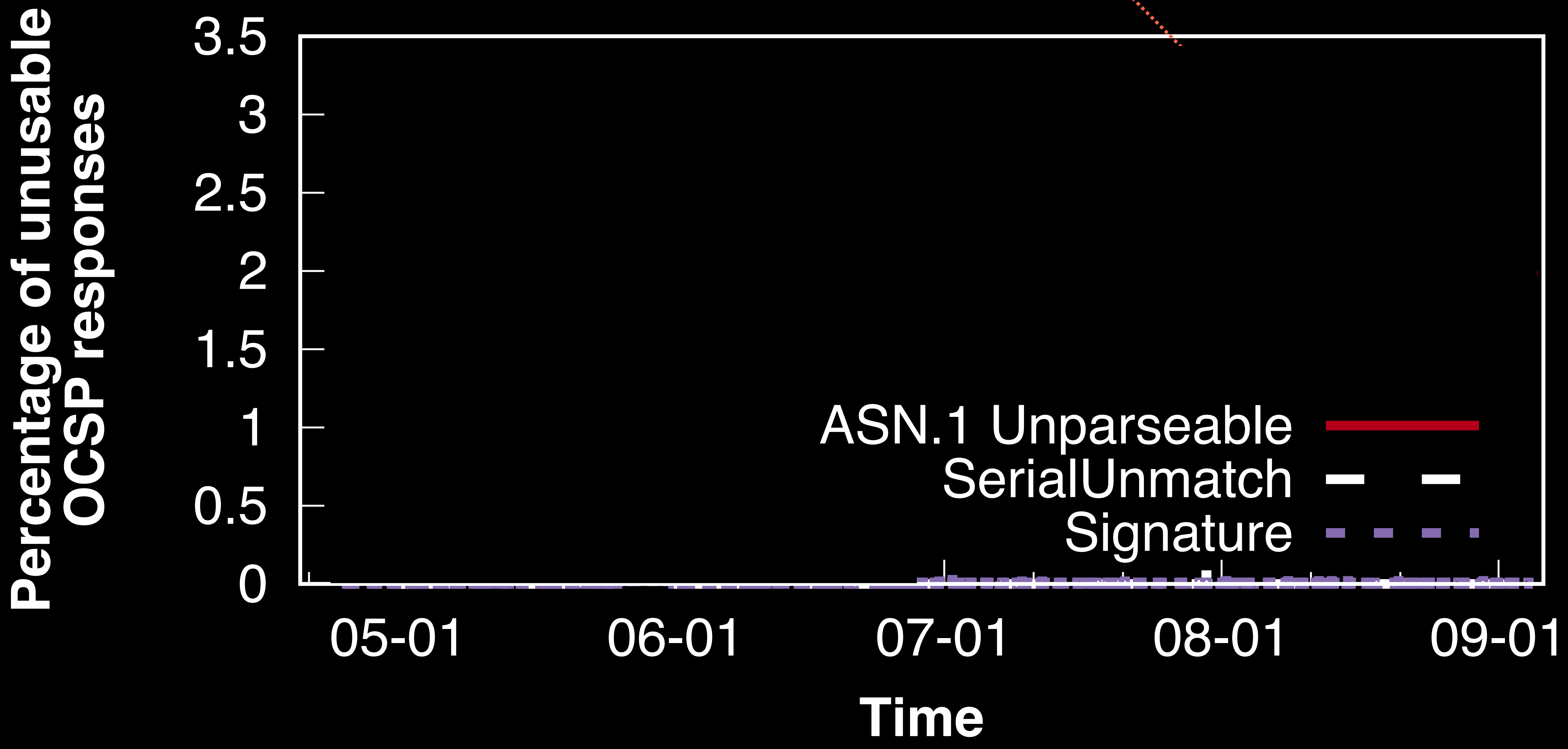


Availability

OCSP responders are not fully reliable

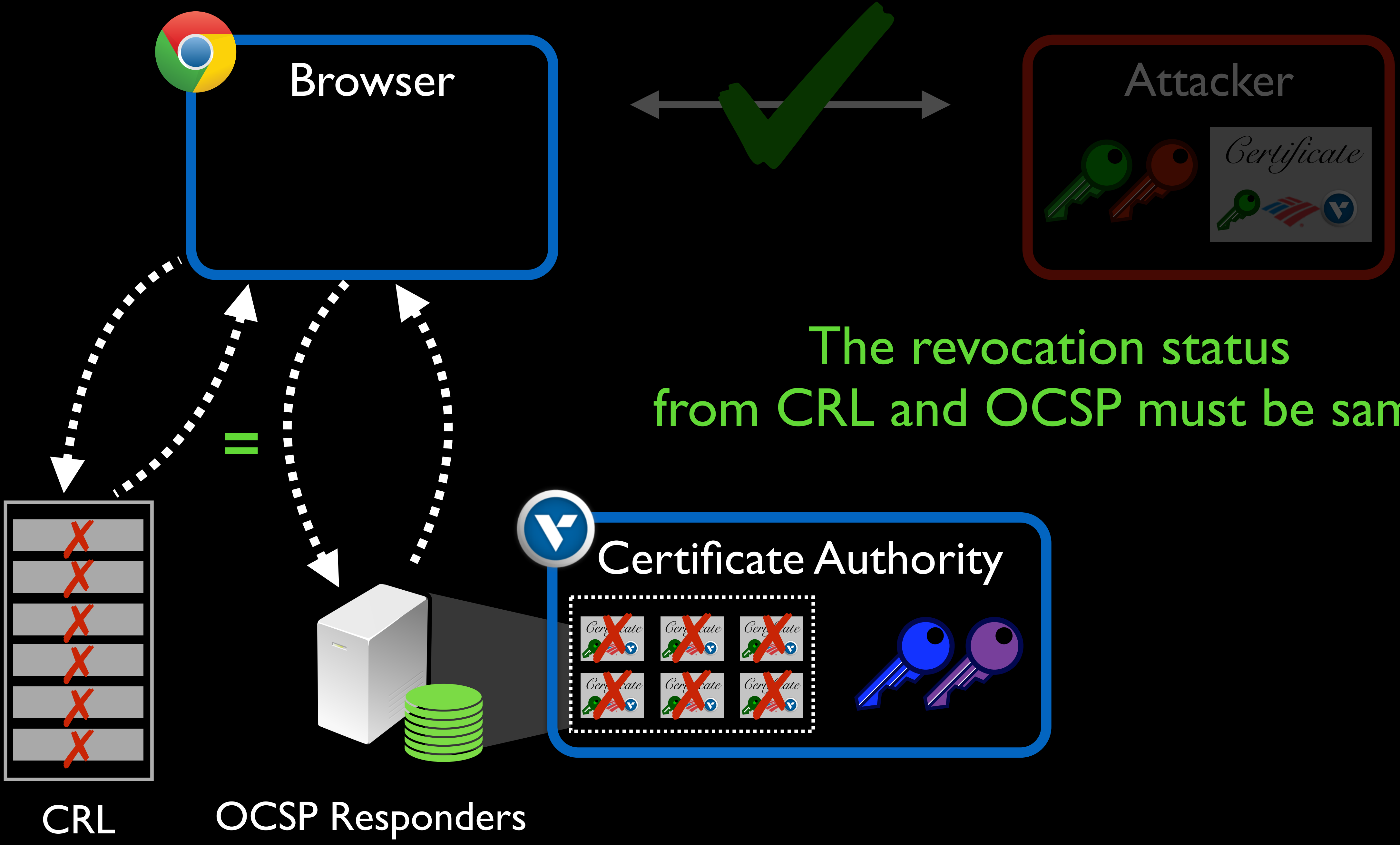
(2) Validity of the Response

3 servers from postsigum.cz
returning "0" response



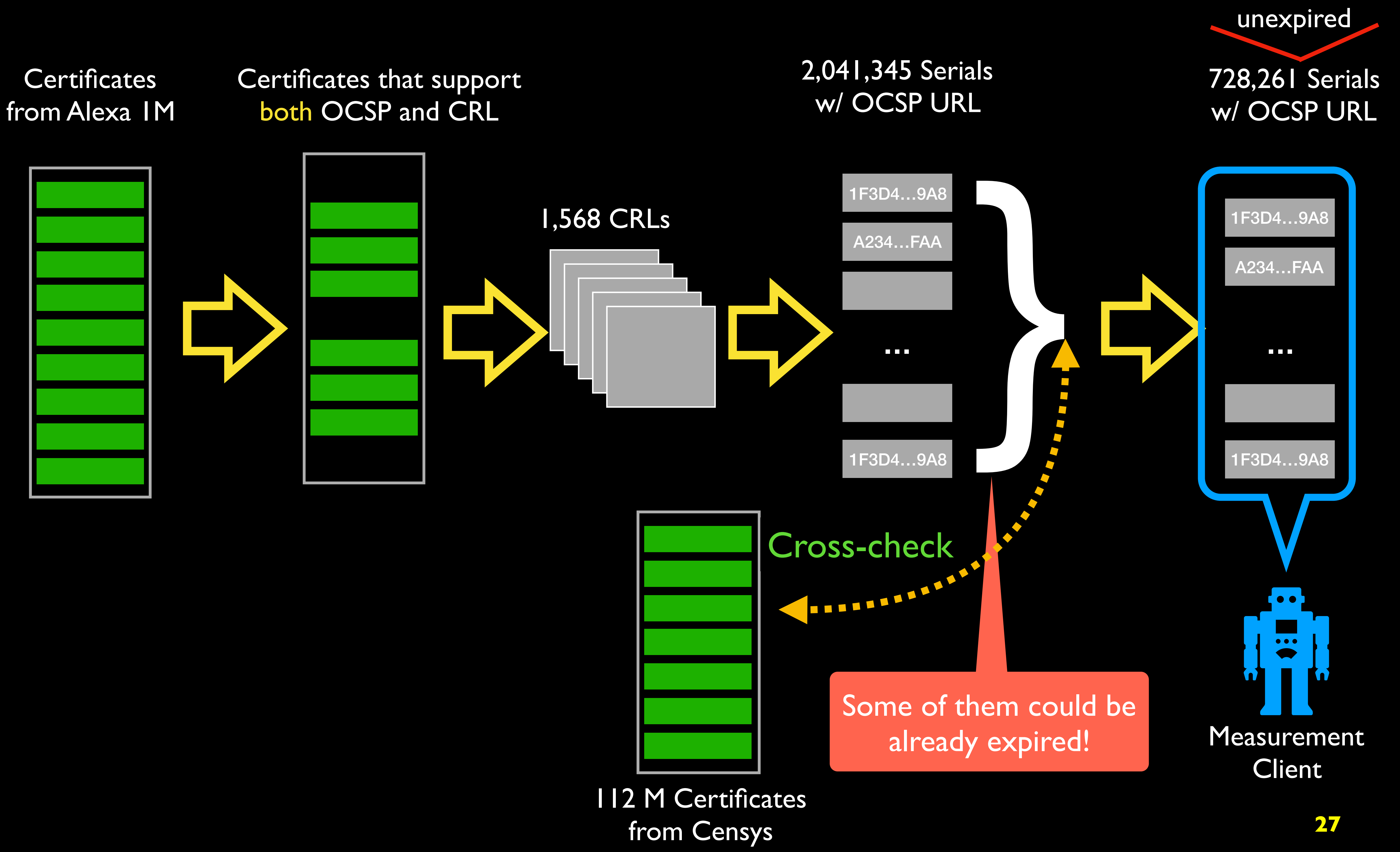
Validity OCSP responses are (mostly) valid

(3) Consistency
OCSP vs. CRL



The revocation status
from CRL and OCSP must be same

(3) Consistency
OCSP vs. CRL


Certificates from Alexa 1M
Certificates that support both OCSP and CRL
1,568 CRLs
2,041,345 Serials w/ OCSP URL
1F3D4…9A8
A234…FAA
…
1F3D4…9A8
unexpired
728,261 Serials w/ OCSP URL
1F3D4…9A8
A234…FAA
…
1F3D4…9A8
Cross-check
112 M Certificates from Censys
Measurement Client

Some of them could be already expired!

(3) Consistency
OCSP vs. CRL

OCSP URL	CRL	# of certificates where the OCSP response is		
		Unknown	Good	Revoked
ocsp.camerfirma.com	crl1.camerfirma.com/camerfirma_cserverii-2015.crl			
ocsp.quovadisglobal.com	crl.quovadisglobal.com/qvsslg3.crl			
ocsp.startssl.com	crl.startssl.com/sca-server1.crl			
ss.symcd.com	ss.symcb.com/ss.crl			
twcasslocsp.twca.com.tw/	sslserver.twca.com.tw/sslserver/securessl			
ocsp2.globalsign.com/gsalphasha2g2	crl2.alphassl.com/gs/gsalphasha2g2.crl			
ocsp.firmaprofesional.com	crl.firmaprofesional.com/infraestructura.crl			
…	…			

(3) Consistency OCSP vs. CRL

OCSP URL	CRL	# of certificates where the OCSP response is		
		Unknown	Good	Revoked
ocsp.camerfirma.com	crl1.camerfirma.com/camerfirma_cserverii-2015.crl	0	7	369
ocsp.quovadisglobal.com	crl.quovadisglobal.com/qvsslg3.crl	0	1	514
ocsp.startssl.com	crl.startssl.com/sca-server1.crl	0	1	[illegible]
ss.symcd.com	ss.symcb.com/ss.crl	0	1	28.032
twcasslocsp.twca.com.tw/	sslserver.twca.com.tw/sslserver/securessl	0	1	122
ocsp2.globalsign.com/gsalphasha2g2	crl2.alphassl.com/gs/gsalphasha2g2.crl	**5.375**	0	0
ocsp.firmaprofesional.com	crl.firmaprofesional.com/infraestructura.crl	**11**	0	0
…	…	0	0	…

*“OCSP and PKI Management are two different platforms and are synchronized by means of some DDBB triggers that are failing in some circumstances. Meanwhile CRL management is easer and simple, OCSP should give information about any certificate serial number issued by *** and the amount of information transmitted between them. That’s the source of this problem.”*

Is the Web Ready for OCSP Must-Staple?

Certificate authority

Web server

Browser

- ✓ Fetch and cache OCSP responses
- ✓ Handling errors

Web Server Methodology

THE APACHE™ SOFTWARE FOUNDATION

NGINX

(1) Performance

? Prefetch OCSP response

(2) Caching

? Cache OCSP response

? Respect nextUpdate* in cache

(3) Availability

? Retain OCSP response on error

*Expiration date of a OCSP response

Web Server Administrator Result

	THE APACHE™ SOFTWARE FOUNDATION	NGINX
Prefetch OCSP response	✗	✗
Cache OCSP response	✓	✓
Respect nextUpdate in cache	✗	✓
Retain OCSP response on error	✗	✓

* Apache version 2.4.18 and Nginx version 1.13.12

Is the Web Ready for OCSP Must-Staple?

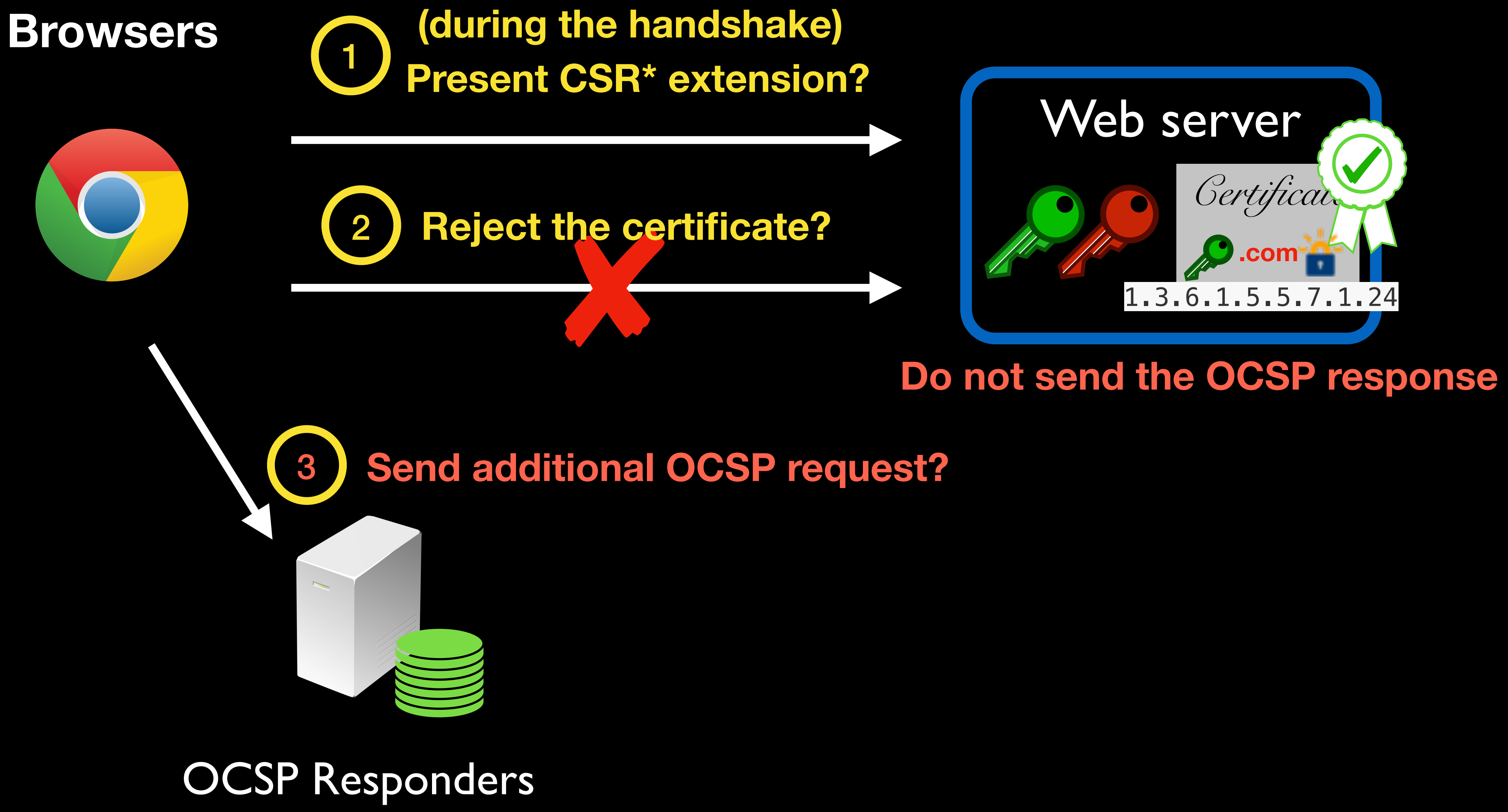
Certificate Authority

Website

Browser

- ✓ Understand the extension
- ✓ Present Certificate Status Request extension
- ✓ Reject the certificate if the response is not provided

Methodology



Browsers

1 (during the handshake) Present CSR* extension?

2 Reject the certificate?

3 Send additional OCSP request?

Do not send the OCSP response

Web server

OCSP Responders

*CSR: Certificate Status Request

Methodology and Result

	Desktop Browsers (OS X, Linux, Windows)						Mobile Browsers			
	Chrome 66	Firefox 60	Opera	Safari	IE	Edge	Safari	Chrome	Firefox/ iOS	Firefox/ Android
Request OCSP Response	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Respect OCSP Must-Staple	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
Send own OCSP Request	✗	-	✗	✗	✗	✗	✗	✗	✗	-

Clients Clients are largely not yet ready for OCSP Must-Staple

(the additional coding work necessary to support OCSP Must-Staple is likely not too significant)

*All tests were done on Ubuntu 16.04, Windows 10, OS X 10.12.6, iOS 11.3, and Android Oreo.

Conclusion

- Considering OCSP Must-Staple can operate only if each of the principals in the PKI performs correctly.
  - OCSP servers: not fully reliable
  - Web server softwares: not fully support
  - Browsers: not fully support
- But the bright side is
  - Only a few players need to take action to make it possible for web server administrators to begin enabling OCSP Must-staple
  - Much wider deployment of OCSP Must-Staple is an realistic and achievable goal

Thanks!

https://securePKI.org

Dataset is available
(we’re still measuring)