



# SSL Research with Bro

Johanna Amann

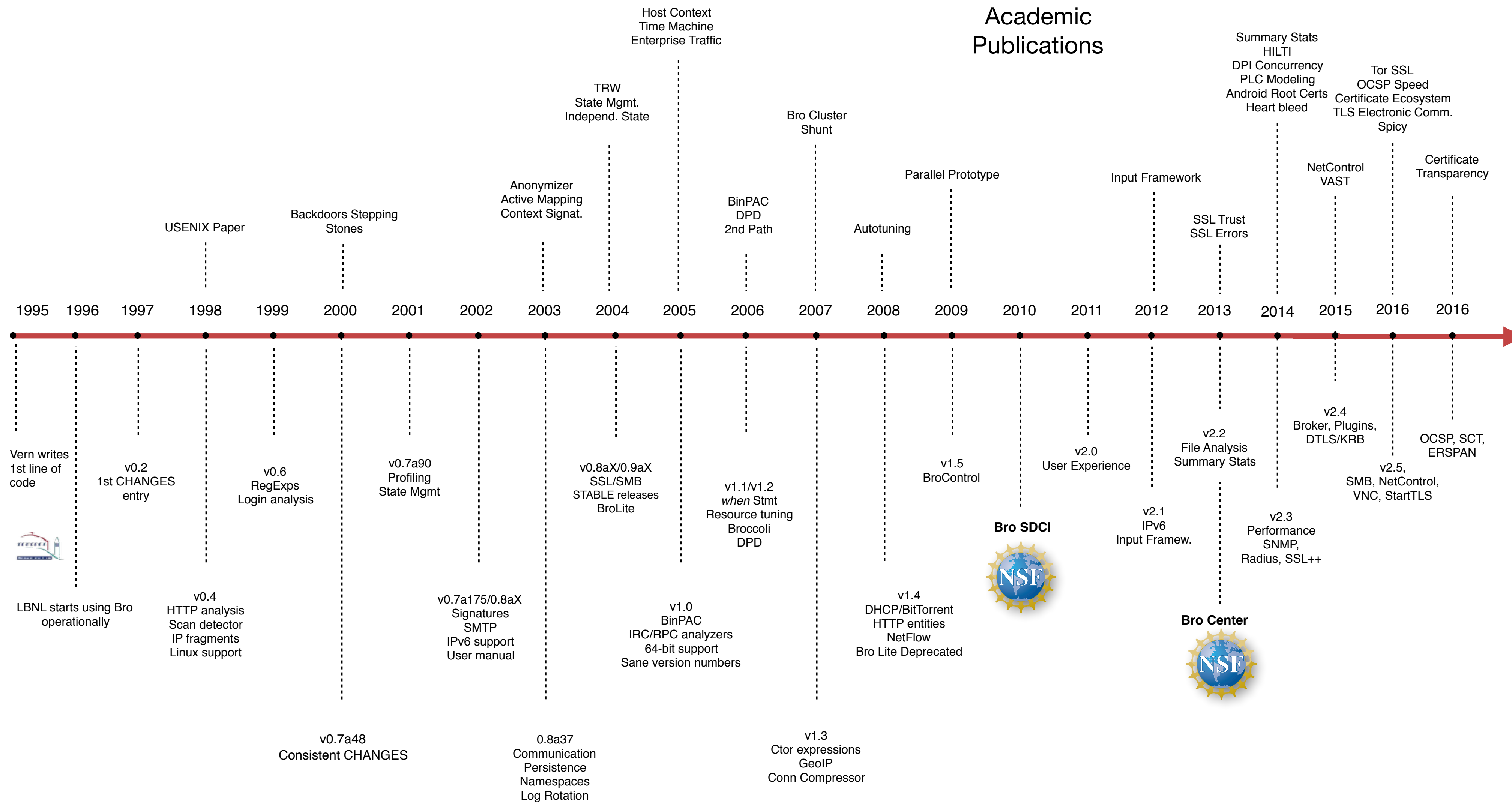
International Computer Science Institute

[johanna@icir.org](mailto:johanna@icir.org)

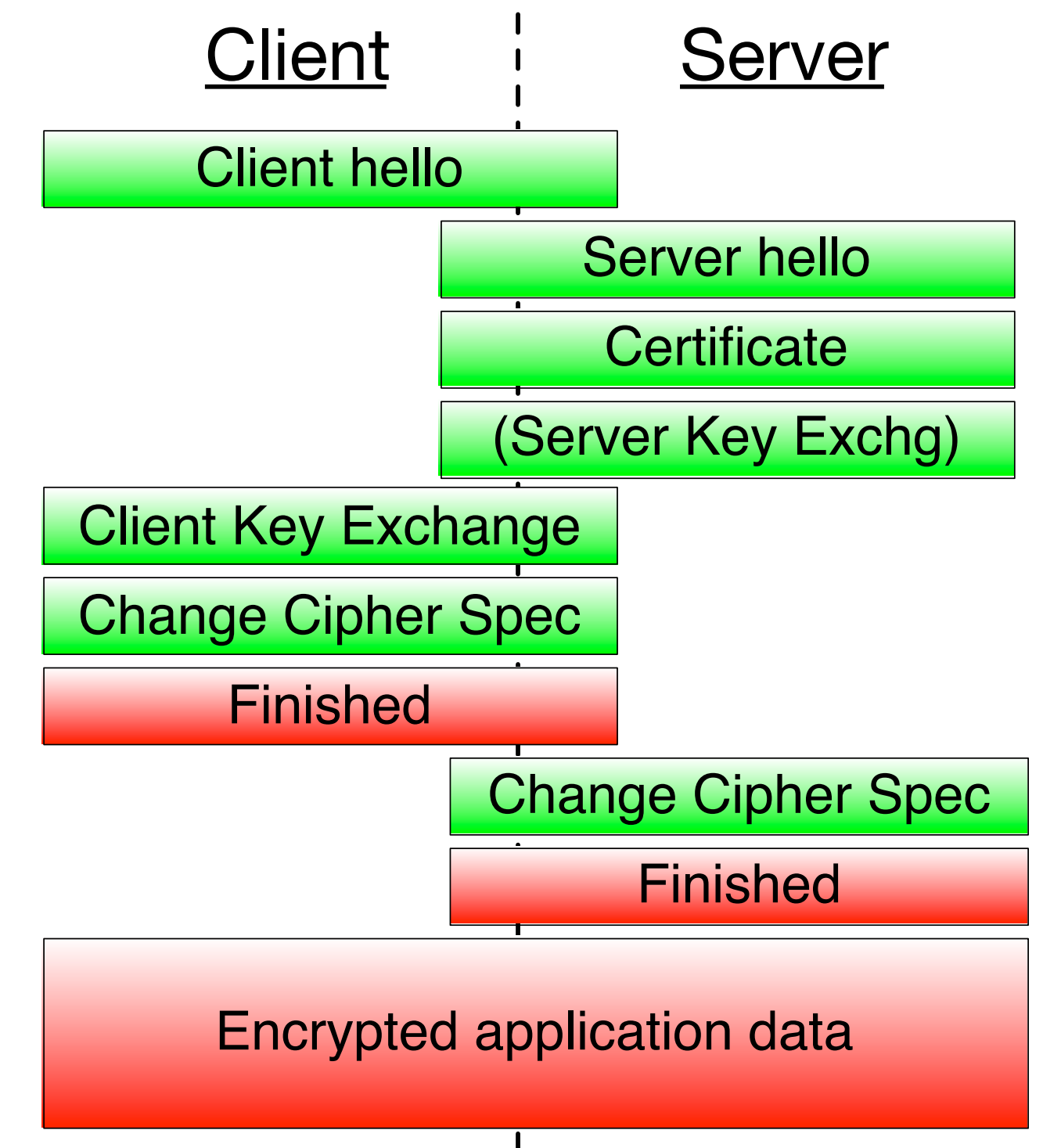
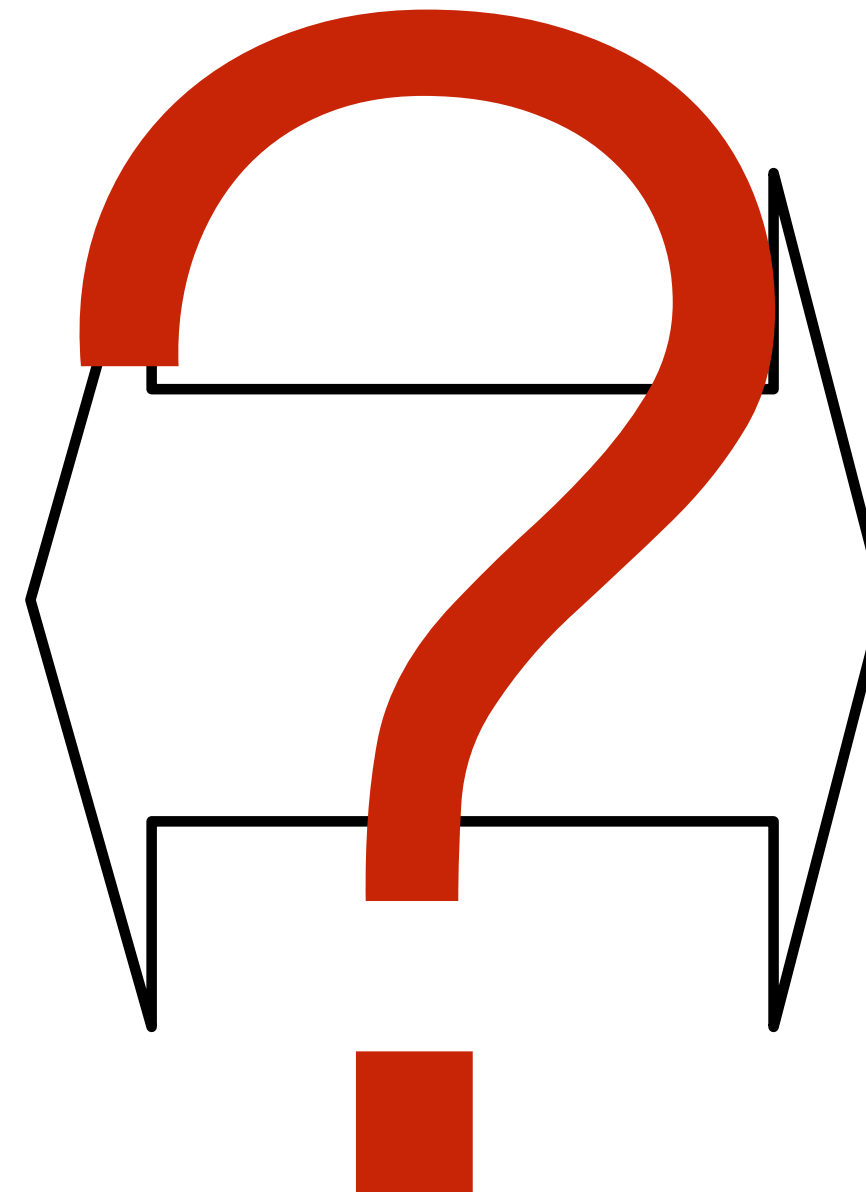
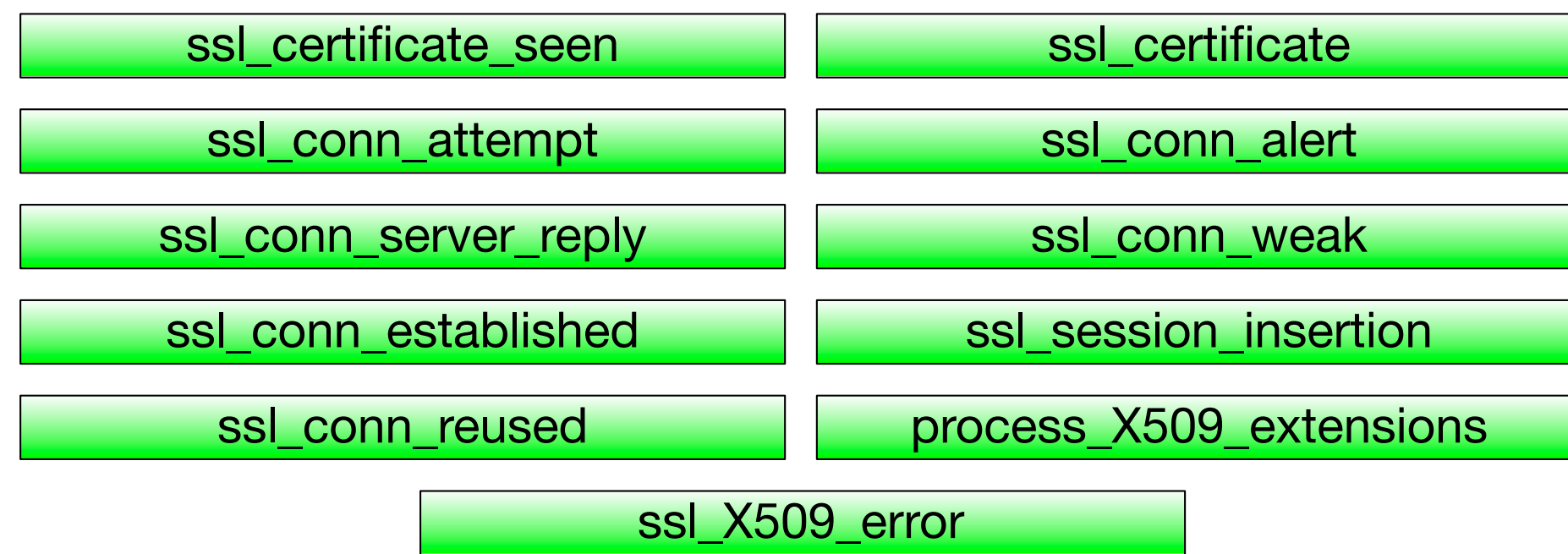
<http://www.icir.org/johanna>



# Bro History



# Bro SSL - v1.5.3



# Bro SSL Events - v2.0 to 2.2

client\_hello

server\_hello

ssl\_session\_ticket\_handshake

ssl\_established

x509\_certificate

ssl\_extension

ssl\_alert



# Bro SSL Events - v2.3

client\_hello

server\_hello

ssl\_session\_ticket\_handshake

ssl\_established

x509\_certificate

ssl\_extension

ssl\_alert

# Bro SSL Events - v2.3

client\_hello

server\_hello

ssl\_session\_ticket\_handshake

ssl\_established

x509\_certificate

ssl\_extension

ssl\_alert

ssl\_stapled\_ocsp

ssl\_encrypted\_data

ssl\_dh\_server\_params

ssl\_change\_cipher\_spec

ssl\_handshake\_message

ssl\_encrypted\_data

ssl\_extension\_ex\_point\_formats

ssl\_server\_curve

ssl\_change\_cipher\_spec

x509\_extension

x509\_ext\_basic\_constraints

x509\_ext\_subject\_alternative\_name

ssl\_extension\_elliptic\_curves

ssl\_extension\_application\_layer\_protocol\_negotiation

ssl\_extension\_server\_name

# Bro SSL Events - v2.4

client\_hello

server\_hello

ssl\_session\_ticket\_handshake

ssl\_established

x509\_certificate

ssl\_extension

ssl\_alert

ssl\_stapled\_ocsp

ssl\_encrypted\_data

ssl\_dh\_server\_params

ssl\_change\_cipher\_spec

ssl\_handshake\_message

ssl\_encrypted\_data

ssl\_extension\_ex\_point\_formats

ssl\_server\_curve

ssl\_change\_cipher\_spec

x509\_extension

x509\_ext\_basic\_constraints

x509\_ext\_subject\_alternative\_name

ssl\_extension\_elliptic\_curves

ssl\_extension\_application\_layer\_protocol\_negotiation

ssl\_extension\_server\_name

# Bro SSL Events - v2.5

client\_hello

server\_hello

ssl\_session\_ticket\_handshake

ssl\_established

x509\_certificate

ssl\_extension

ssl\_alert

ssl\_stapled\_ocsp

ssl\_encrypted\_data

ssl\_dh\_server\_params

ssl\_change\_cipher\_spec

ssl\_handshake\_message

ssl\_encrypted\_data

ssl\_extension\_ex\_point\_formats

ssl\_server\_curve

ssl\_change\_cipher\_spec

x509\_extension

x509\_ext\_basic\_constraints

x509\_ext\_subject\_alternative\_name

ssl\_extension\_elliptic\_curves

ssl\_extension\_application\_layer\_protocol\_negotiation

ssl\_extension\_server\_name



# Bro SSL Events - v2.5

client\_hello

server\_hello

ssl\_session\_ticket\_handshake

ssl\_established

x509\_certificate

ssl\_extension

ssl\_alert

ssl\_stapled\_ocsp

ssl\_encrypted\_data

ssl\_dh\_server\_params

ssl\_change\_cipher\_spec

ssl\_handshake\_message

ssl\_encrypted\_data

ssl\_extension\_ex\_point\_formats

ssl\_server\_curve

ssl\_change\_cipher\_spec

x509\_extension

x509\_ext\_basic\_constraints

x509\_ext\_subject\_alternative\_name

ssl\_extension\_elliptic\_curves

ssl\_extension\_application\_layer\_protocol\_negotiation

ssl\_extension\_server\_name

ssl\_extension\_signature\_algorithm

# Bro SSL Events - v2.5

Completely working DTLS support

More StartTLS

TLS 1.3 support

ssl\_change\_cipher\_spec

x509\_extension

x509\_ext\_basic\_constraints

x509\_ext\_subject\_alternative\_name

ssl\_extension\_elliptic\_curves

ssl\_extension

ssl\_encrypted\_data

ssl\_extension\_application\_layer\_protocol\_negotiation

ssl\_alert

ssl\_extension\_ex\_point\_formats

ssl\_extension\_server\_name

ssl\_server\_curve

ssl\_extension\_signature\_algorithm

# Bro SSL Events - master

client\_hello

server\_hello

ssl\_session\_ticket\_handshake

ssl\_established

x509\_certificate

ssl\_extension

ssl\_alert

ssl\_stapled\_ocsp

ssl\_encrypted\_data

ssl\_dh\_server\_params

ssl\_change\_cipher\_spec

ssl\_handshake\_message

ssl\_encrypted\_data

ssl\_extension\_ex\_point\_formats

ssl\_server\_curve

ssl\_change\_cipher\_spec

x509\_extension

x509\_ext\_basic\_constraints

x509\_ext\_subject\_alternative\_name

ssl\_extension\_elliptic\_curves

ssl\_extension\_application\_layer\_protocol\_negotiation

ssl\_extension\_server\_name

ssl\_extension\_signature\_algorithm

# Bro SSL Events - master

client\_hello

server\_hello

ssl\_session\_ticket\_handshake

ssl\_established

x509\_certificate

ssl\_extension

ssl\_alert

ssl\_server\_curve

ssl\_extension\_supported\_versions

ocsp\_request

ocsp\_response\_bytes

ssl\_stapled\_ocsp

ssl\_encrypted\_data

ssl\_dh\_server\_params

ssl\_change\_cipher\_spec

ssl\_handshake\_message

ssl\_encrypted\_data

ssl\_extension\_ex\_point\_formats

ssl\_extension\_signature\_algorithm

ssl\_extension\_psk\_key\_exchange\_modes

ocsp\_request\_certificate

ocsp\_response\_certificate

ssl\_change\_cipher\_spec

x509\_extension

x509\_ext\_basic\_constraints

x509\_ext\_subject\_alternative\_name

ssl\_extension\_elliptic\_curves

ssl\_extension\_application\_layer\_protocol\_negotiation

ssl\_extension\_server\_name

x509\_ocsp\_ext\_signed\_certificate\_timestamp

ssl\_extension\_signed\_certificate\_timestamp

ocsp\_response\_status

ocsp\_extension



# Bro SSL Events - master

client\_hello

ssl\_stapled\_ocsp

ssl\_change\_cipher\_spec

server\_hello

ssl\_encrypted\_data

x509\_extension

OCSP support

SCT Support (Certificate Transparency)

TLS 1.3 extensions

ms

x509\_ext\_basic\_constraints

spec

x509\_ext\_subject\_alternative\_name

sage

ssl\_extension\_elliptic\_curves

ta

ssl\_extension\_application\_layer\_protocol\_negotiation

\_formats

ssl\_extension\_server\_name

ssl\_server\_curve

ssl\_extension\_signature\_algorithm

x509\_ocsp\_ext\_signed\_certificate\_timestamp

ssl\_extension\_supported\_versions

ssl\_extension\_psk\_key\_exchange\_modes

ssl\_extension\_signed\_certificate\_timestamp

ocsp\_request

ocsp\_request\_certificate

ocsp\_response\_status

ocsp\_response\_bytes

ocsp\_response\_certificate

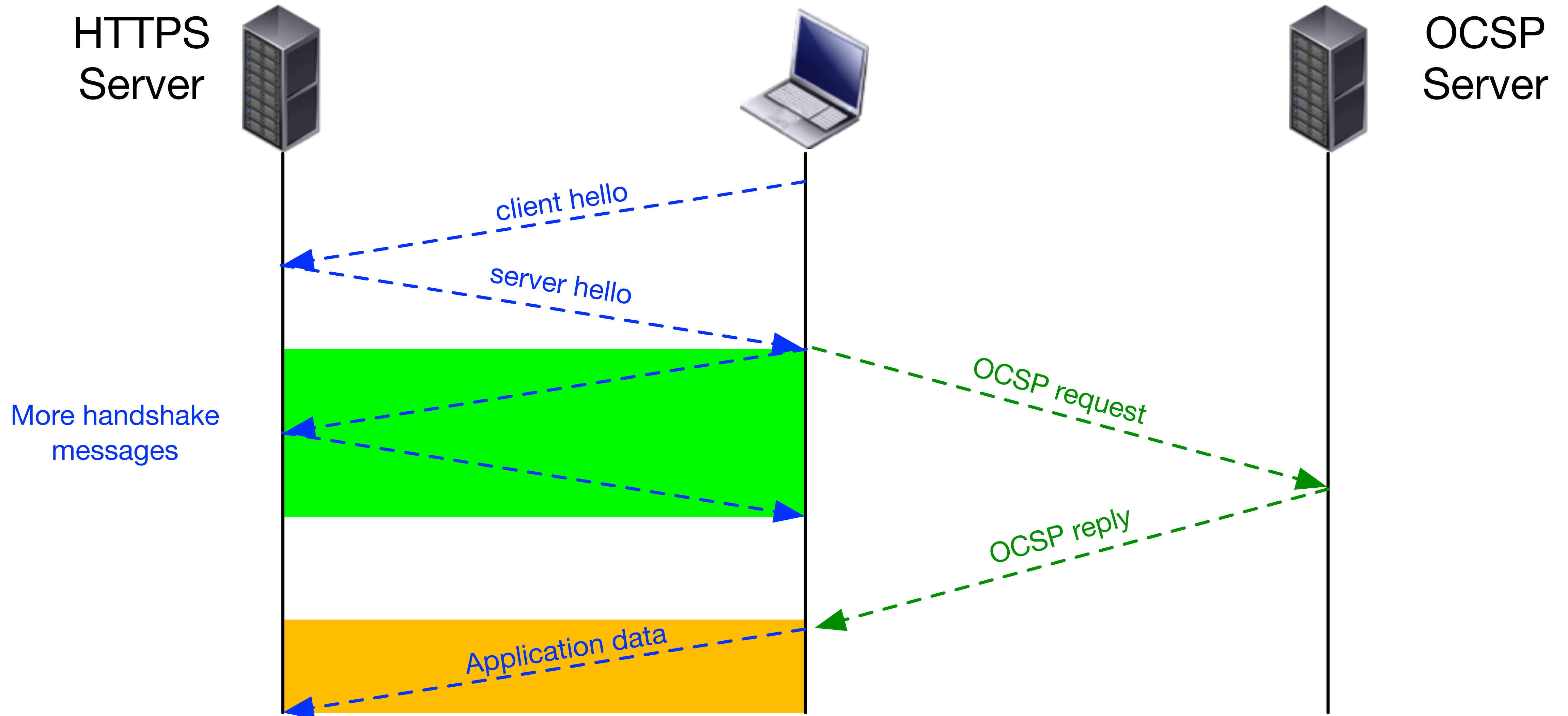
ocsp\_extension



# TLS 1.3

<b>ts</b>	1505018739.255782
<b>id.resp_h</b>	104.19.196.102
<b>version</b>	TLSv13-draft18
<b>cipher</b>	TLS_AES_128_GCM_SHA256
<b>curve</b>	x25519
<b>server_name</b>	<u>tls13.cloudflare.com</u>
<b>established</b>	T
<b>cert_chain_fuids</b>	-
<b>client_cert_chain_fuids</b>	-
<b>subject</b>	-
<b>issuer</b>	-

# OCSP



# @load files/x509/log-ocsp

<b>ts</b>	1438374033.033189
<b>id</b>	FVty9v3KTnCvbg0Xf2
<b>hashAlgorithm</b>	sha1
<b>issuerNameHash</b>	74241467069FF5E0983F5E3E1A6BA0652A541575
<b>issuerKeyHash</b>	0159ABE7DD3A0B59A66463D6CF200757D591E76A
<b>serialNumber</b>	017447CB30072EE15B9C1B057B731C5A
<b>certStatus</b>	revoked
<b>revoketime</b>	1421494379.000000
<b>revokereason</b>	keyCompromise
<b>thisUpdate</b>	1436321024.000000
<b>nextUpdate</b>	1443459307.000000

# Certificate Transparency

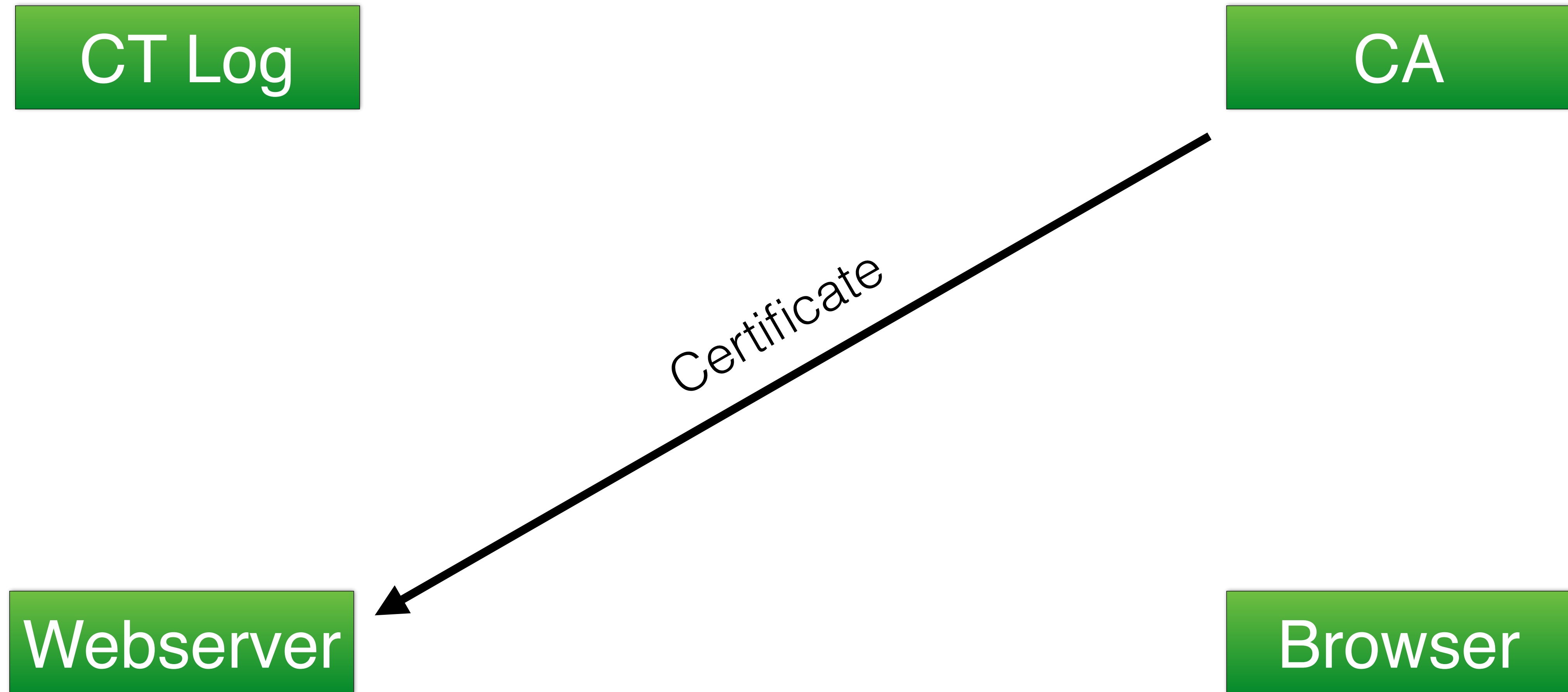
CT Log

CA

Webserver

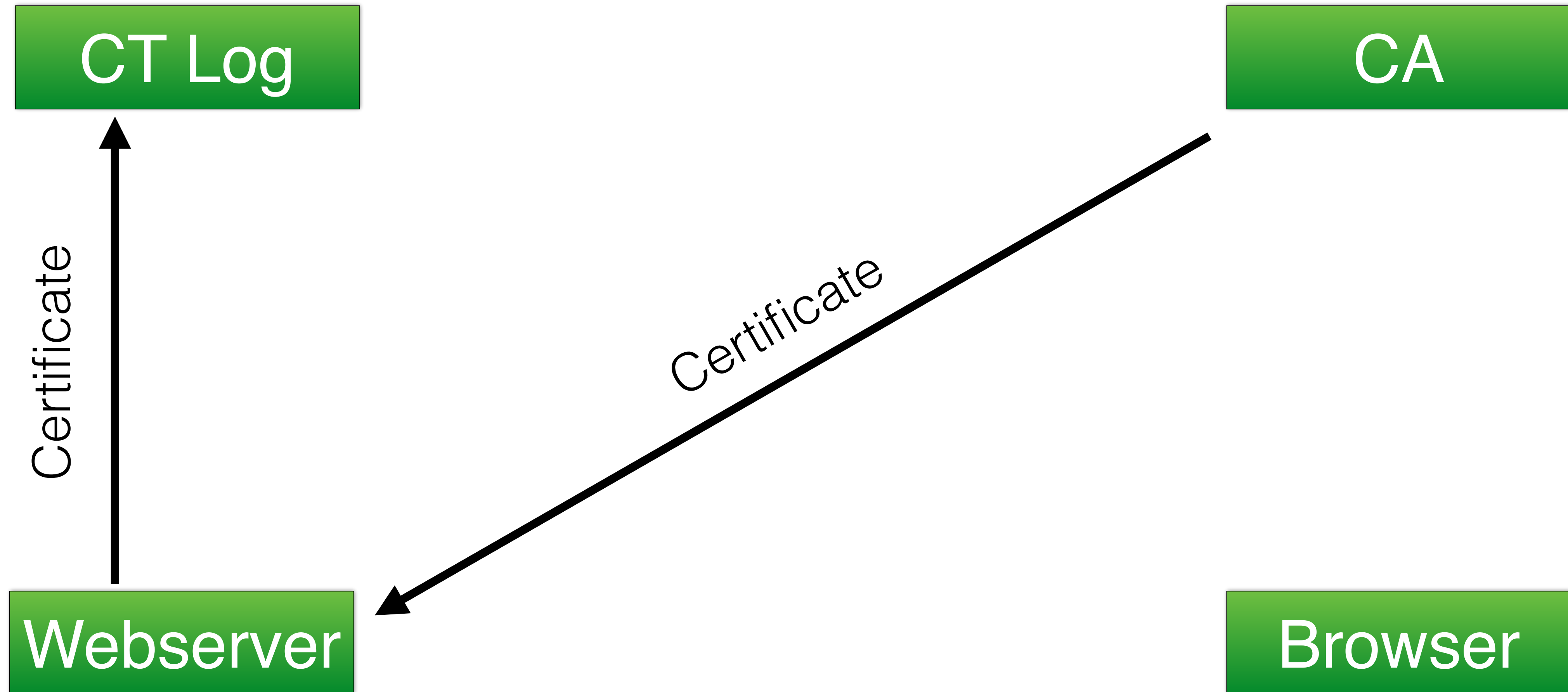
Browser

# Certificate Transparency

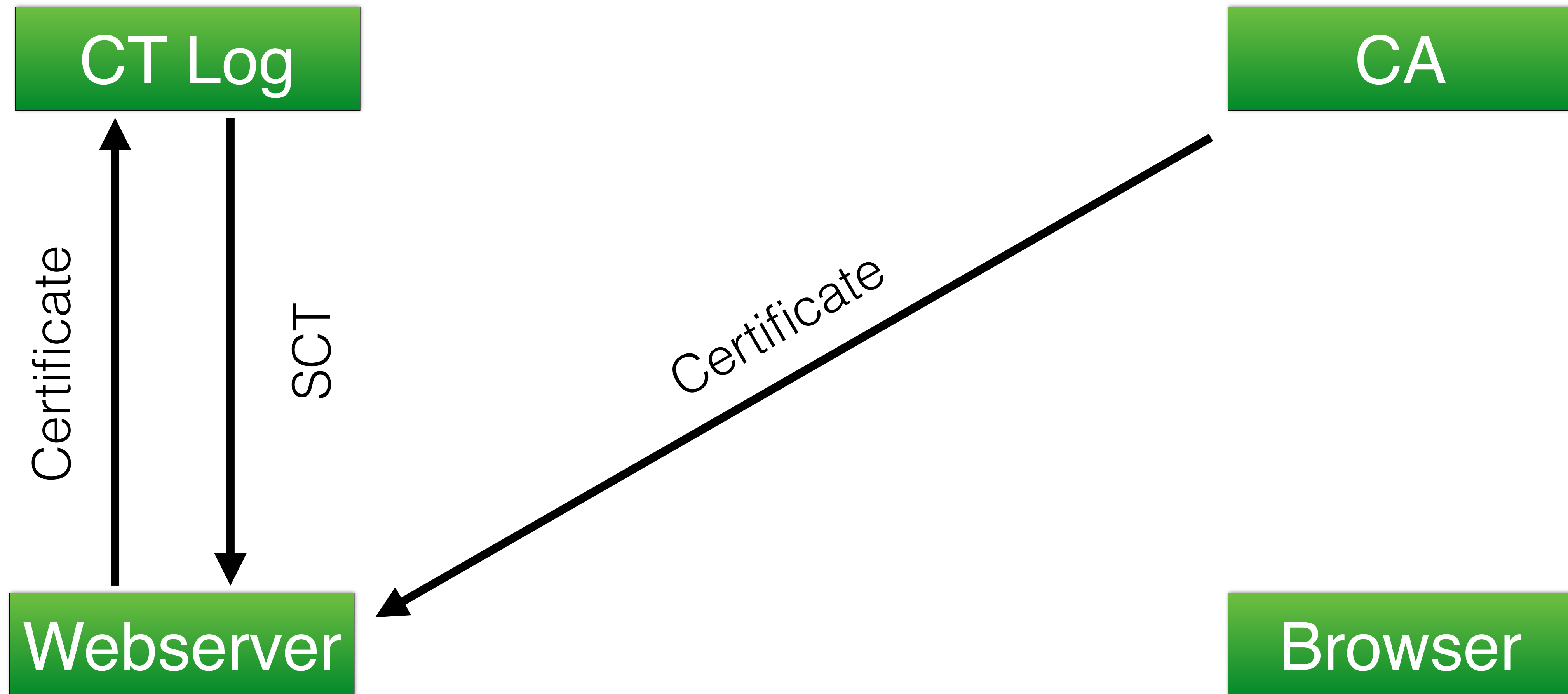




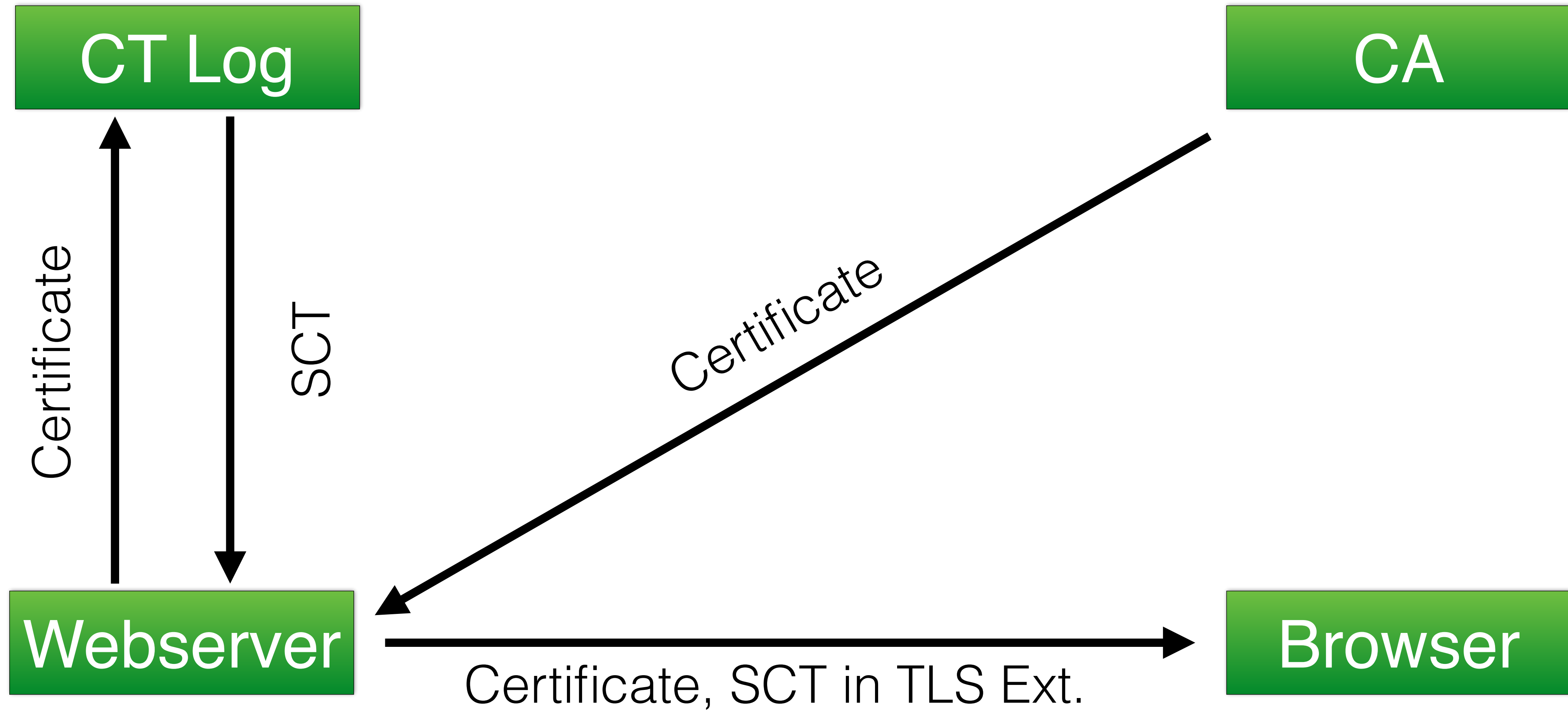
# Certificate Transparency



# Certificate Transparency



# Certificate Transparency



# Certificate Transparency

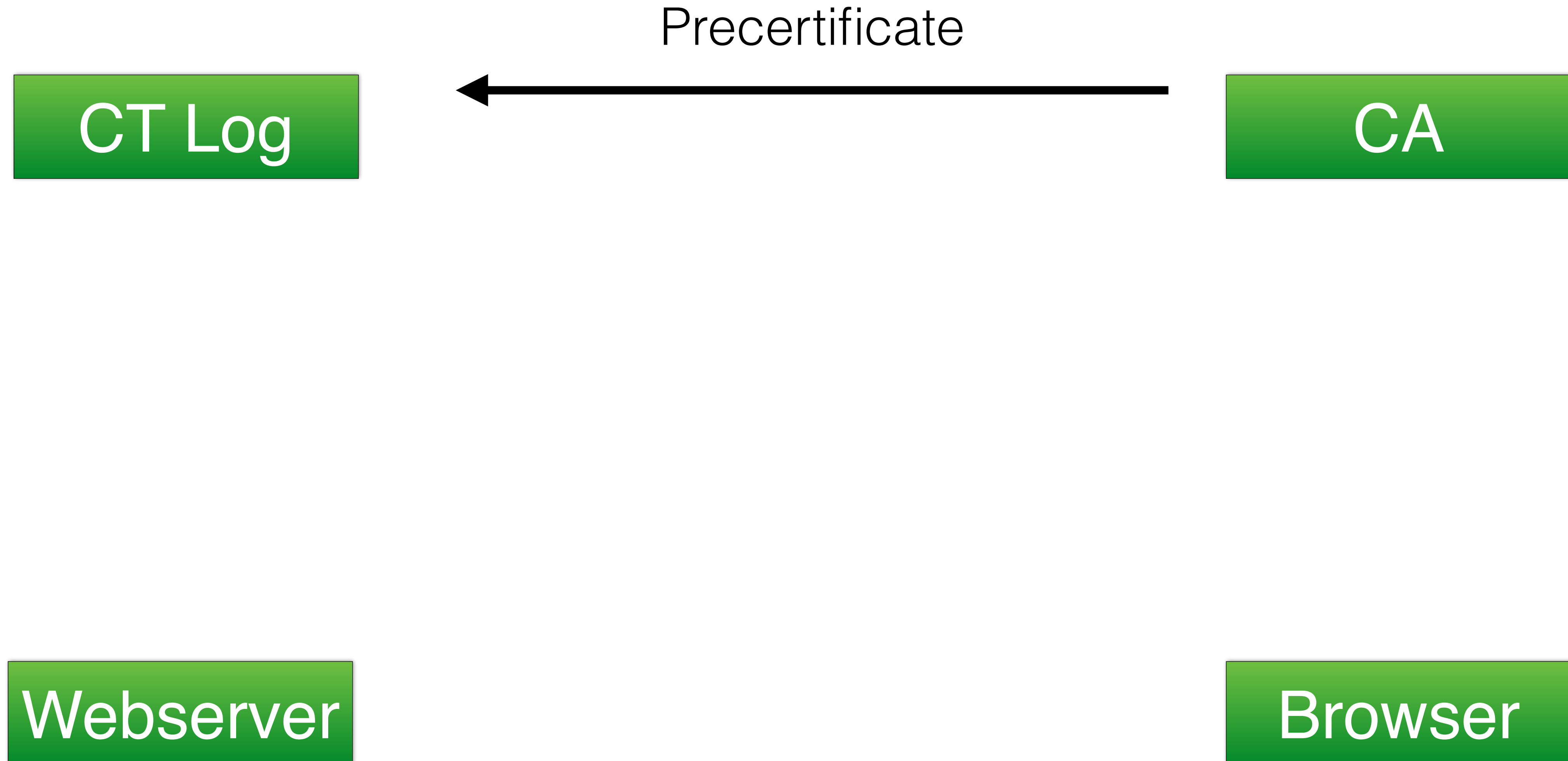
CT Log

CA

Webserver

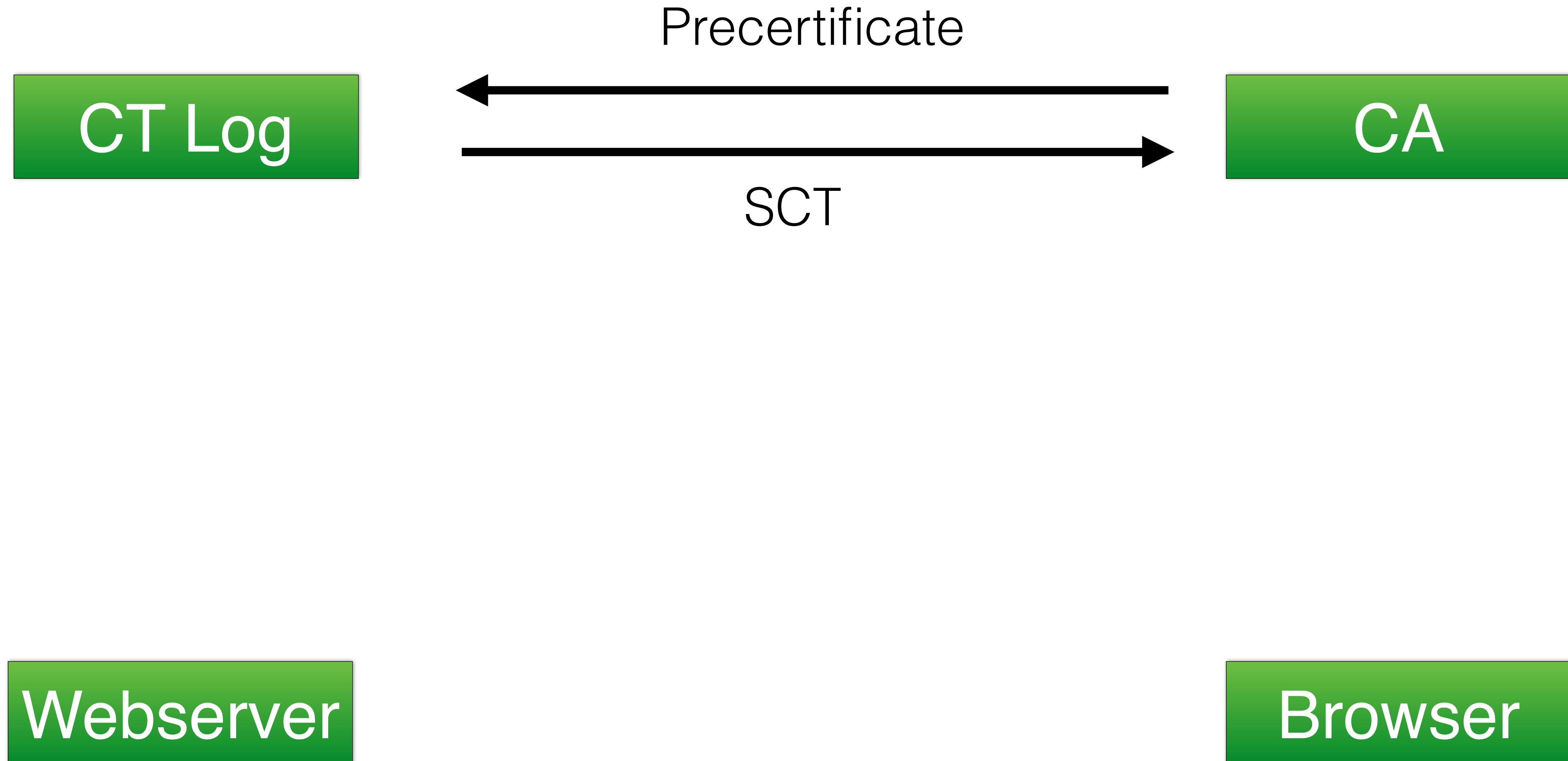
Browser

# Certificate Transparency

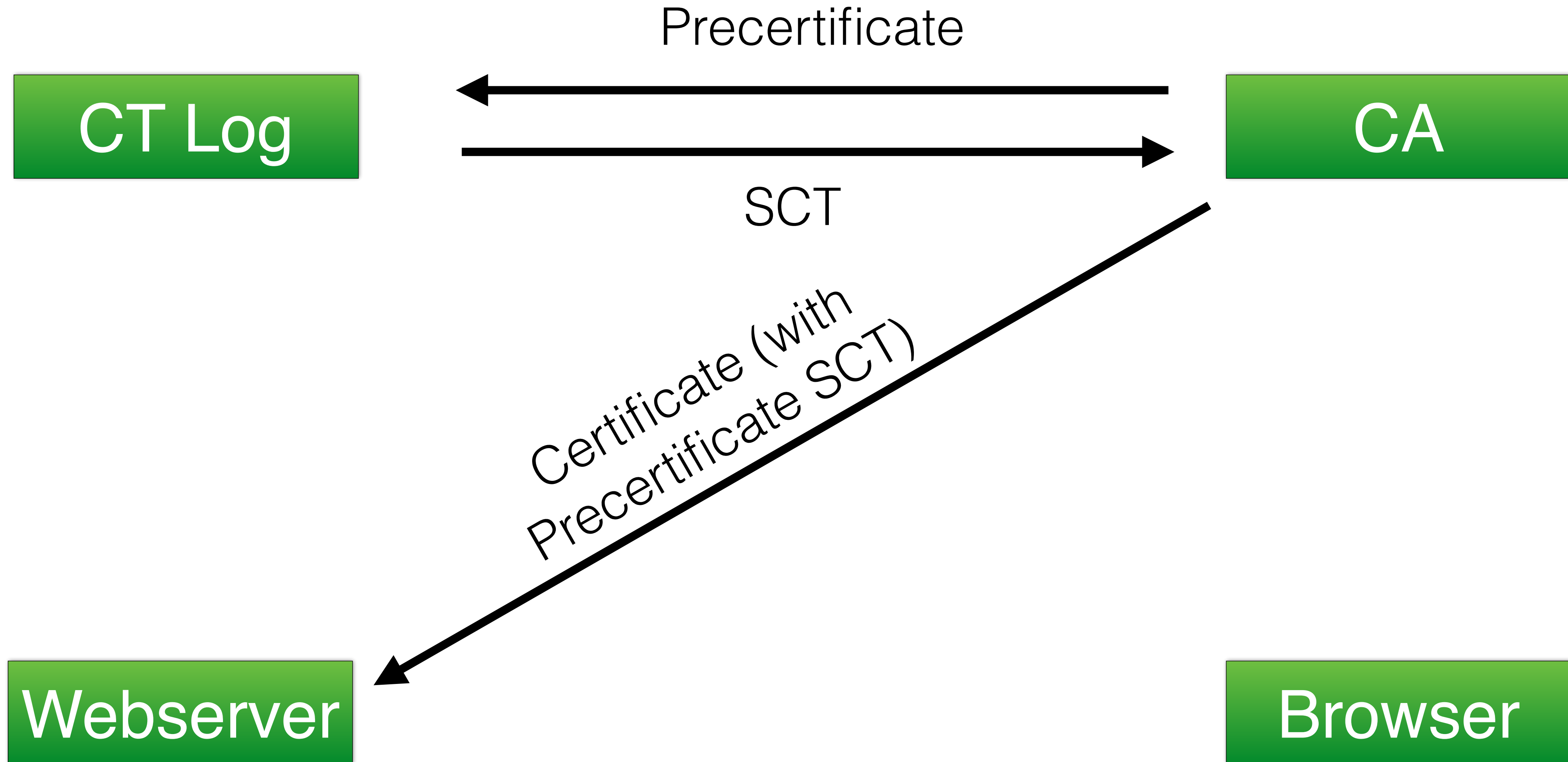




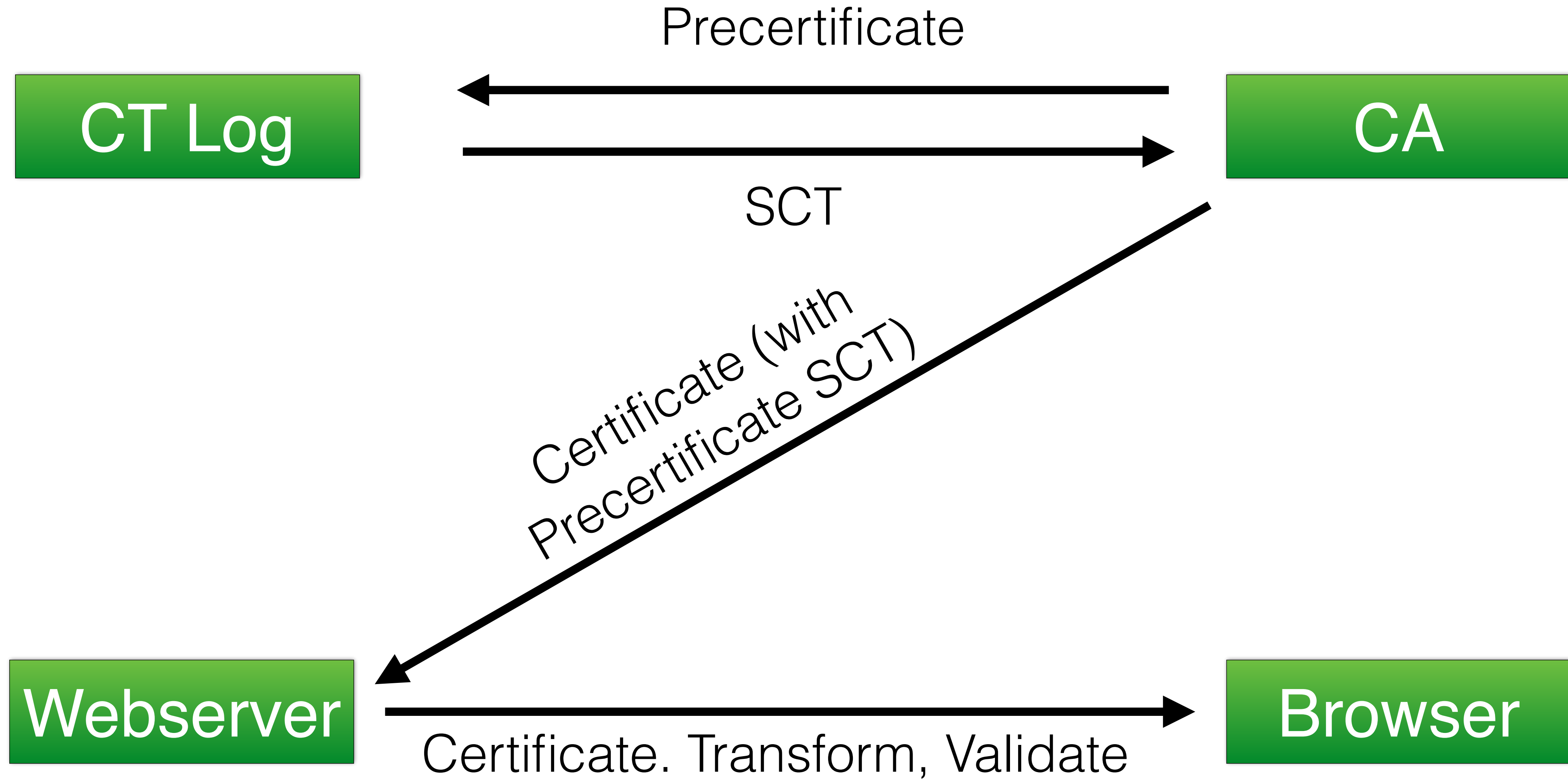
# Certificate Transparency



# Certificate Transparency



# Certificate Transparency



# Certificate Transparency

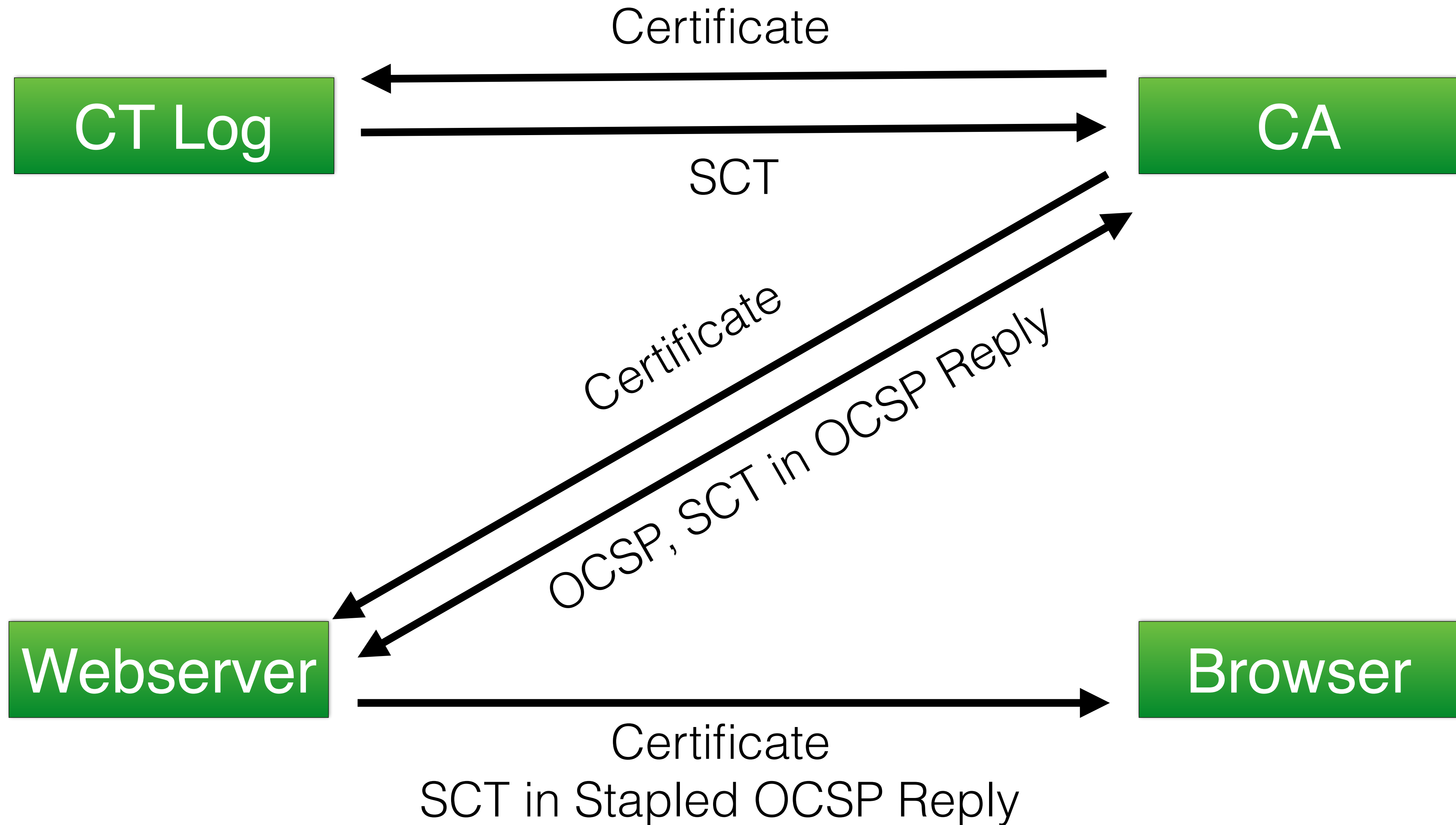
CT Log

CA

Webserver

Browser

# Certificate Transparency





# TLS Versions

The screenshot displays a web browser window with the address bar showing `Secure https://www.wsgvet.com`. The page is in Korean. The Chrome DevTools Security panel is open, showing the Certificate Transparency section. The list of SCT logs includes:

- SCT Symantec log (Embedded in certificate, Verified)
- SCT DigiCert Log Server (Embedded in certificate, Verified)
- SCT Google 'Aviator' log (Embedded in certificate, Verified)
- SCT Google 'Pilot' log (Embedded in certificate, Verified)
- SCT Google 'Rocketeer' log (Embedded in certificate, Verified)
- SCT Google 'Rocketeer' log (TLS extension, Verified)
- SCT Google 'Aviator' log (TLS extension, Verified)
- SCT Symantec log (TLS extension, Verified)
- SCT WoSign log (TLS extension, Verified)
- SCT Venafi log (TLS extension, Verified)
- SCT Google 'Skydiver' log (TLS extension, Verified)
- SCT DigiCert Log Server (TLS extension, Verified)
- SCT Google 'Pilot' log (TLS extension, Verified)

The page content shows a blog post titled "가든스 바이 더 베이 플라워 돔 (3) - 싱가포르 첫 번째 여행기 #17".



# TLS Versions

WOMAGazine-ウーマガジン- x

Secure <https://womagazine.jp>

This page is in Japanese Would you like to translate it? [Nope](#) [Translate](#) Options x

WOMAGazine

ホーム ダイエット 美容 ファッション

休日に足を運んで食べに行きたいっ♪  
最旬の「抹茶スイーツ」が食べられる  
お店をご紹介します...

1699 Views

5月5日の注目記事

出会いは美BODYが  
引き寄せる!?1ヶ月  
10キロも可能な痩身  
エステで、見事別人

寝坊しても大丈夫！  
「10分」でかわいく  
なれる簡単メイク術

Overview

Main Origin

- https://womagazine.jp

Non-Secure Origins

- chrome-extension://nffaoalbilbmmfgebngppjih

Secure Origins

- https://www.google-analytics.com
- https://uh.nakanohito.jp
- https://pagead2.googlesyndication.com
- https://platform.twitter.com
- https://connect.facebook.net
- https://googleads.g.doubleclick.net

Subject womagazine.jp

SAN womagazine.jp  
www.womagazine.jp

Valid From Sat, 22 Apr 2017 17:07:00 GMT

Valid Until Fri, 21 Jul 2017 17:07:00 GMT

Issuer Let's Encrypt Authority X3

[Open full certificate details](#)

Certificate Transparency

- SCT Google 'Rocketeer' log (TLS extension, Invalid signature)
- SCT Google 'Pilot' log (TLS extension, Invalid signature)

[Show full details](#)

The security details above are from the first inspected response.

Console What's New x

Highlights from Chrome 59 update

CSS and JS code coverage  
Find unused CSS and JS with the new Coverage drawer.

Full-page screenshots  
Take a screenshot of the entire page, from the top of the viewport to the bottom.

Block requests  
Manually disable individual requests in the Network panel.

URL	Type	Total Bytes	Unused Bytes	Unused %
/script_foot_close	JS	385 983	250 341	65.2 %
/query_ui-bundle	JS	241 682	217 071	89.8 %
ht.../script_foot.js	JS	231 291	156 748	67.8 %
https://develop...	CS...	185 663	122 783	66.1 %
/devsite-google-tr	CSS	129 754	104 360	80.4 %
/ss=AAZnThnRE	JS	138 015	98 170	71.1 %
/cb-gapi_loaded_1	JS	122 005	81 366	66.7 %
h/query-bundle.js	JS	88 065	43 956	50.0 %
/css?family=Robo	CSS	23 967	23 616	98.5 %
https://di.../di.js	JS	31 249	20 270	64.9 %
...	...	...	...	...

# TLS Versions

The screenshot shows a browser window with three tabs: Netflix, Folkehelseinstituttet - FHI, and Nginx Forum. The address bar shows a secure connection to <https://forum.nginx.org>. The page content includes the Nginx logo, a search bar, and forum announcements. The Chrome DevTools Security panel is open, showing the certificate chain for the domain. The main origin is <https://forum.nginx.org>, and a secure origin is <https://ssl.google-analytics.com>. The certificate details include:

- Subject: forum.nginx.org
- SAN: forum.nginx.org
- Valid From: Mon, 10 Apr 2017 12:48:00 GMT
- Valid Until: Sun, 09 Jul 2017 12:48:00 GMT
- Issuer: Let's Encrypt Authority X3

Certificate Transparency (SCT) logs are listed below:

- SCT Google 'Rocketeer' log (TLS extension, Verified)
- SCT Google 'Pilot' log (TLS extension, Verified)
- SCT WoSign log (TLS extension, Invalid signature)
- SCT Google 'Icarus' log (TLS extension, Verified)

A note at the bottom of the security panel states: "The security details above are from the first inspected response." Below the security panel, the Chrome DevTools console shows "Highlights from Chrome 59 update" with sections for CSS and JS code coverage, Full-page screenshots, and Block requests. A table of resource loading statistics is also visible:

LURL	Type	Total Bytes	Unused Bytes
/script_foot_closu	JS	385 563	256 341 66.2 %
/query_ui-bundle	JS	241 682	217 071 89.8 %
ht.../script_foot.js	JS	231 291	156 748 67.8 %
https://develo...	CS...	185 563	122 783 66.1 %
/devsite-google-bi	CSS	129 754	104 360 80.4 %
/js=AAZYrThiYEG	JS	138 015	88 170 71.1 %
/cb=gapi.loaded_1	JS	122 055	81 366 66.7 %
h/jquery-bundle.js	JS	88 065	43 996 50.0 %
/ce?family=Robo	CSS	23 867	23 616 98.5 %
https://dl.../dn.js	JS	31 249	20 270 64.8 %
ext/orig-res	JS	52 021	7 154 13.7 %



# TLS Versions

105 Certificates, 91 Let's Encrypt

The screenshot shows a web browser window with three tabs: Netflix, Folkehelseinstituttet - FHI, and Nginx Forum. The address bar shows a secure connection to https://forum.nginx.org. A yellow box highlights the text '105 Certificates, 91 Let's Encrypt'. The Security panel is open, showing the following details:

- Subject: forum.nginx.org
- SAN: forum.nginx.org
- Valid From: Mon, 10 Apr 2017 12:48:00 GMT
- Valid Until: Sun, 09 Jul 2017 12:48:00 GMT
- Issuer: Let's Encrypt Authority X3

Below the main details, there is a section for Certificate Transparency with the following entries:

- SCT: Google 'Rocketeer' log (TLS extension, Verified)
- SCT: Google 'Pilot' log (TLS extension, Verified)
- SCT: WoSign log (TLS extension, Invalid signature)
- SCT: Google 'Icarus' log (TLS extension, Verified)

A 'Show full details' link is present below the SCT entries. A note at the bottom of the Security panel states: 'The security details above are from the first inspected response.'

The browser's console shows a 'What's New' notification for Chrome 59 update, listing features like 'CSS and JS code coverage', 'Full-page screenshots', and 'Block requests'. A table of resource loading statistics is also visible in the bottom right corner of the console area.

LURL	Type	Total Bytes	Unused Bytes
/script_foot_closu	JS	385 563	256 341 66.2 %
/query_ui-bundle	JS	241 682	217 071 89.8 %
ht.../script_foot.js	JS	231 291	156 748 67.8 %
https://develop...	CS...	185 563	122 783 66.1 %
/devsite-google-bi	CSS	129 754	104 360 80.4 %
/is-AAZYrThvYE2	JS	138 015	88 170 71.1 %
/cb-gapi_loaded_1	JS	122 055	81 366 66.7 %
h/jquery-bundle.js	JS	88 065	43 996 50.0 %
/ce?family=Robo	CSS	23 867	23 616 98.5 %
https://dl.../dn.js	JS	31 249	20 270 64.8 %
ext/ios/...	JS	52 021	7 154 37.7 %

# TLS Versions

Folkehelseinstituttet - FHI

Secure <https://www.fhi.no>

This page is in Norwegian Would you like to translate it? [Nope](#) [Translate](#) Options

Elements Console Sources Network Performance Memory Application **Security** Audits

Overview

Main Origin

- <https://www.fhi.no>

Secure Origins

- <https://www.google-analytics.com>
- <https://www.googletagmanager.com>
- <https://www.googleadservices.com>
- <https://connect.facebook.net>
- <https://googleads.g.doubleclick.net>
- <https://www.google.com>
- <https://www.facebook.com>

Unknown / Canceled

- <https://code.jquery.com>

Subject [www.fhi.no](https://www.fhi.no)

SAN [www.fhi.no](https://www.fhi.no)  
[admin.fhi.no](https://admin.fhi.no)  
[Show more \(4 total\)](#)

Valid From Thu, 09 Jun 2016 12:32:36 GMT

Valid Until Sat, 09 Jun 2018 21:59:00 GMT

Issuer Buypass Class 3 CA 2

[Open full certificate details](#)

Certificate Transparency

- SCT Google 'Aviator' log (Embedded in certificate, Invalid signature)
- SCT Venafi log (Embedded in certificate, Invalid signature)
- SCT Symantec log (Embedded in certificate, Invalid signature)

[Show full details](#)

The security details above are from the first inspected response.

# @load protocols/ssl/validate-sct.bro

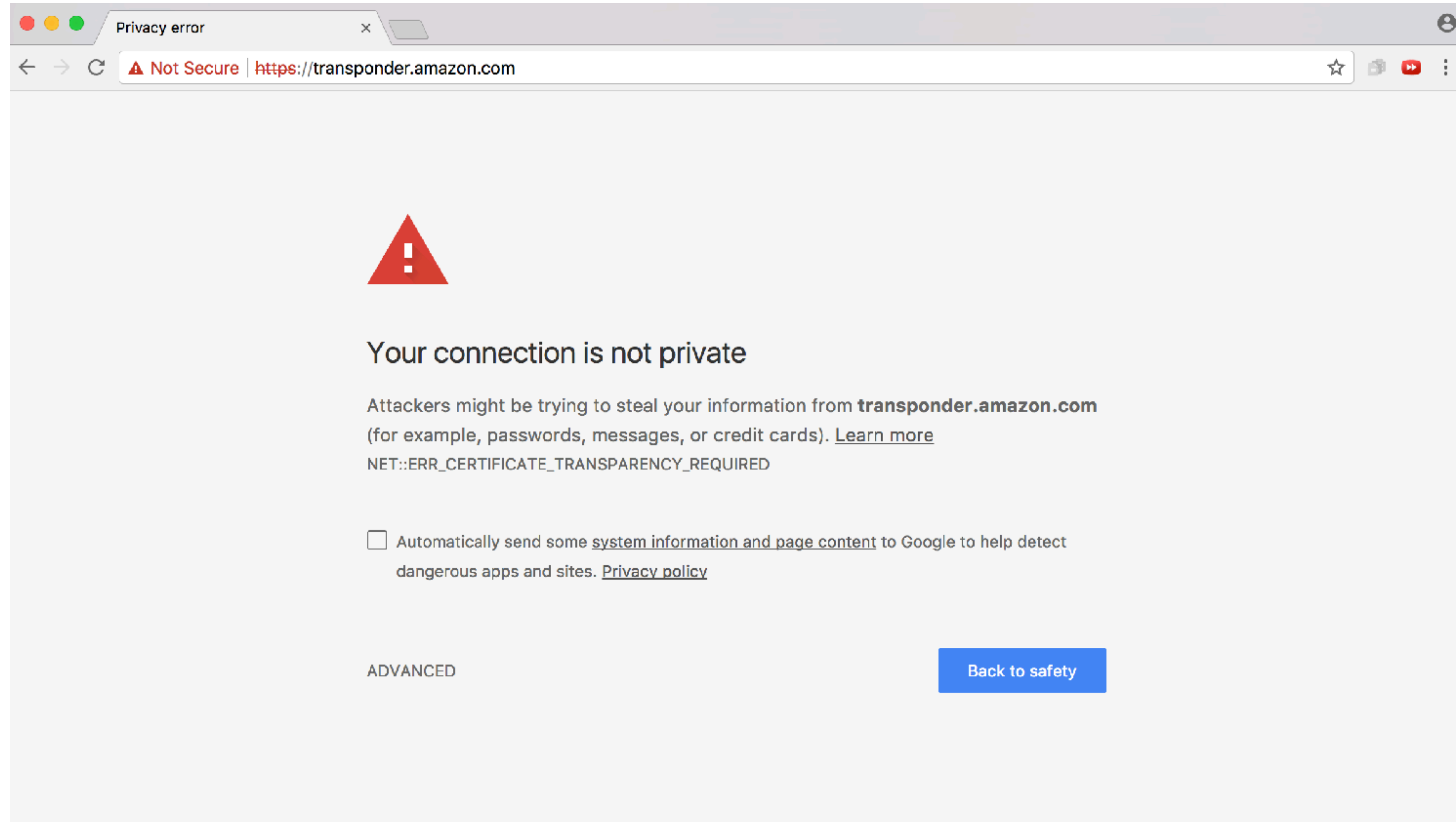
<b>ts</b>	1484228945.191472
<b>id.resp_h</b>	97.107.139.108
<b>version</b>	TLSv12
<b>cipher</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
<b>curve</b>	secp256r1
<b>server_name</b>	ritter.vg
<b>subject</b>	CN=ritter.vg,OU=PositiveSSL,OU=Domain...
<b>issuer</b>	CN=COMODO RSA Domain Validation Secure...
<b>validation_status</b>	ok
<b>valid_ct_logs</b>	3
<b>valid_ct_operators</b>	1



# Log Operators

Active	Passive
Symantec log (81.26%)	Symantec log (62.78%)
Google 'Pilot' log (79.9%)	Google 'Rocketeer' log (58.6%)
Google 'Rocketeer' log (31.72%)	Google 'Pilot' log (58.48%)
DigiCert Log Server (26.96%)	Google 'Icarus' log (14.37%)
Google 'Aviator' log (25.67%)	Google 'Aviator' log (9.39%)
Google 'Skydiver' log (8.32%)	Vena log (7.47%)
Symantec VEGA log (3.98%)	WoSign ctlog (4.64%)
StartCom CT log (1.49%)	DigiCert Log Server (4.07%)
WoSign ctlog (0.67%)	Google 'Skydiver' log (1.7%)

# Log Operators



# SCT Statistics

	CA	Munich	Sydney
<b>Time</b>	4/4-5/2	5/12-5/16	5/12-5/16
<b>Conns</b>	2.6G	287M	196M
<b>Conns with SCT</b>	779M	73M	58M
<b>... in Cert</b>	520M	58M	44M
<b>... in TLS</b>	248M	14M	14M
<b>... in OCSP</b>	156K	38K	31K
<b>Total IPv4</b>	737K	344K	226K
<b>SCT IP</b>	222K	102K	66K

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

36:9a:c7:3d:67:06:3a:a2:75:83:0d:fc:66:84:1c:1e

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4

Validity

Not Before: May 30 00:00:00 2016 GMT

Not After : May 30 00:00:00 2018 GMT

Subject: C=US, ST=Washington, L=Seattle, O=Amazon.com, Inc., CN=\*.cloudfront.net

X509v3 extensions:

X509v3 Subject Alternative Name:

DNS:cloudfront.net, DNS:\*.cloudfront.net

X509v3 Basic Constraints:

CA:FALSE

Authority Information Access:

OCSP - URI:http://ss.symcd.com

CA Issuers - URI:http://ss.symcb.com/ss.crt

CT Precertificate SCTs:

..Random string goes here

```
853:d=5 hl=2 l= 3 prim: OBJECT :X509v3 CRL Distribution Points
858:d=5 hl=2 l= 36 prim: OCTET STRING [HEX DUMP]:30223020A01EA01C861A687474703A2F2F73732E73796D63622E636F6D2F73732E63726C
896:d=4 hl=2 l= 87 cons: SEQUENCE
898:d=5 hl=2 l= 8 prim: OBJECT :Authority Information Access
908:d=5 hl=2 l= 75 prim: OCTET STRING [HEX DUMP]:3049301F06082B060105050730018613687474703A2F2F73732E73796D63642E636F6D30260
063622E636F6D2F73732E637274
985:d=4 hl=2 l= 39 cons: SEQUENCE
987:d=5 hl=2 l= 10 prim: OBJECT :CT Precertificate SCTs
999:d=5 hl=2 l= 25 prim: OCTET STRING [HEX DUMP]:0C1752616E646F6D20737472696E6720676F65732068657265
```

```
853:d=5 hl=2 l= 3 prim: OBJECT :X509v3 CRL Distribution Points
858:d=5 hl=2 l= 36 prim: OCTET STRING [HEX DUMP]:30223020A01EA01C861A687474703A2F2F73732E73796D63622E636F6D2F73732E63726C
896:d=4 hl=2 l= 87 cons: SEQUENCE
898:d=5 hl=2 l= 8 prim: OBJECT :Authority Information Access
908:d=5 hl=2 l= 75 prim: OCTET STRING [HEX DUMP]:3049301F06082B060105050730018613687474703A2F2F73732E73796D63642E636F6D30260
063622E636F6D2F73732E637274
985:d=4 hl=2 l= 39 cons: SEQUENCE
987:d=5 hl=2 l= 10 prim: OBJECT :CT Precertificate SCTs
999:d=5 hl=2 l= 25 prim: OCTET STRING [HEX DUMP]:0C1752616E646F6D20737472696E6720676F65732068657265
```

```
$ openssl asn1parse -in invalidsct.crt -inform der -strparse 999
 0:d=0 hl=2 l= 23 prim: UTF8STRING :Random string goes here
```



# Normal SCT

CT Precertificate SCTs:

Signed Certificate Timestamp:

Version : v1(0)  
Log ID : DD:EB:1D:2B:7A:0D:4F:A6:20:8B:81:AD:81:68:70:7E:  
2E:8E:9D:01:D5:5C:88:8D:3D:11:C4:CD:B6:EC:BE:CC  
Timestamp : Aug 17 17:25:11.747 2016 GMT  
Extensions: none  
Signature : ecdsa-with-SHA256  
30:46:02:21:00:B9:6C:2B:9A:D5:C8:70:EC:CD:2E:17:  
E6:69:5E:C0:51:47:24:D5:DE:37:CF:10:54:84:A7:D6:  
FD:6B:A4:A6:31:02:21:00:ED:0C:E0:49:63:60:D7:26:  
DD:DD:06:B4:80:D6:42:FC:F4:C5:74:70:C5:4F:4D:8D:  
9F:41:61:91:BB:B1:73:86

Signed Certificate Timestamp:

Version : v1(0)  
Log ID : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:  
3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10  
Timestamp : Aug 17 17:25:11.810 2016 GMT  
Extensions: none  
Signature : ecdsa-with-SHA256  
30:45:02:21:00:C4:A9:7D:4B:93:C1:57:BB:AF:39:01:  
D9:5B:CB:01:35:44:97:7A:9B:E9:FD:A2:F7:15:CA:F2:  
16:4B:88:5E:AC:02:20:10:9D:1E:54:8D:3A:C1:20:65:  
A9:25:BE:8F:00:8E:26:26:2D:D8:E7:BA:AE:48:84:19:  
35:86:0D:B8:EC:B3:D4



Certificate:

Data:

Version: 3 (0x2)

Serial Number:

36:9a:c7:3d:67:06:3a:a2:75:83:0d:fc:66:84:1c:1e

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4

Validity

Not Before: May 30 00:00:00 2016 GMT

Not After : May 30 00:00:00 2018 GMT

Subject: C=US, ST=Washington, L=Seattle, O=Amazon.com, Inc., CN=\*.cloudfront.net

X509v3 extensions:

X509v3 Subject Alternative Name:

DNS:cloudfront.net, DNS:\*.cloudfront.net

X509v3 Basic Constraints:

CA:FALSE

Authority Information Access:

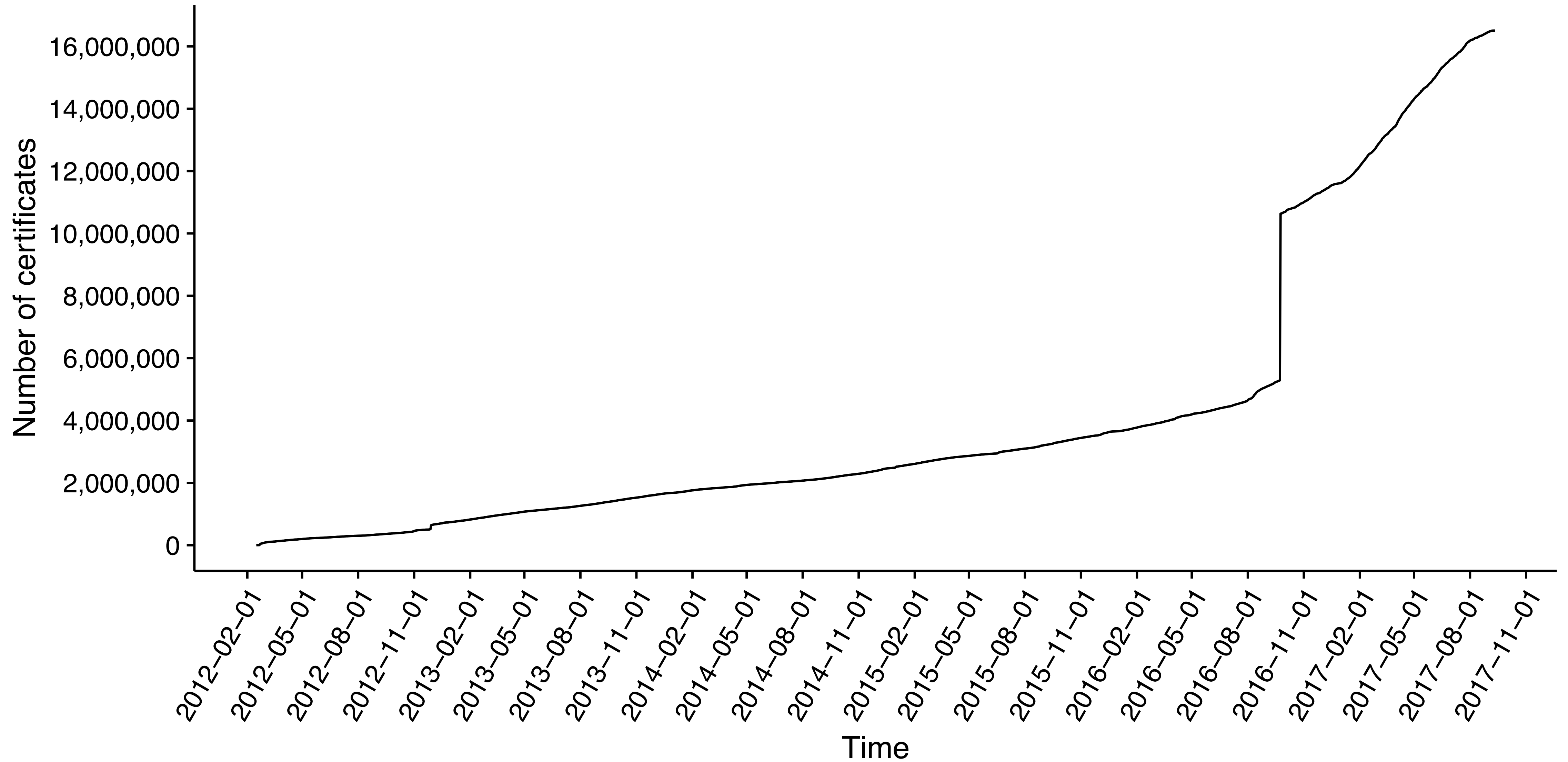
OCSP - URI:http://ss.symcd.com

CA Issuers - URI:http://ss.symcb.com/ss.crt

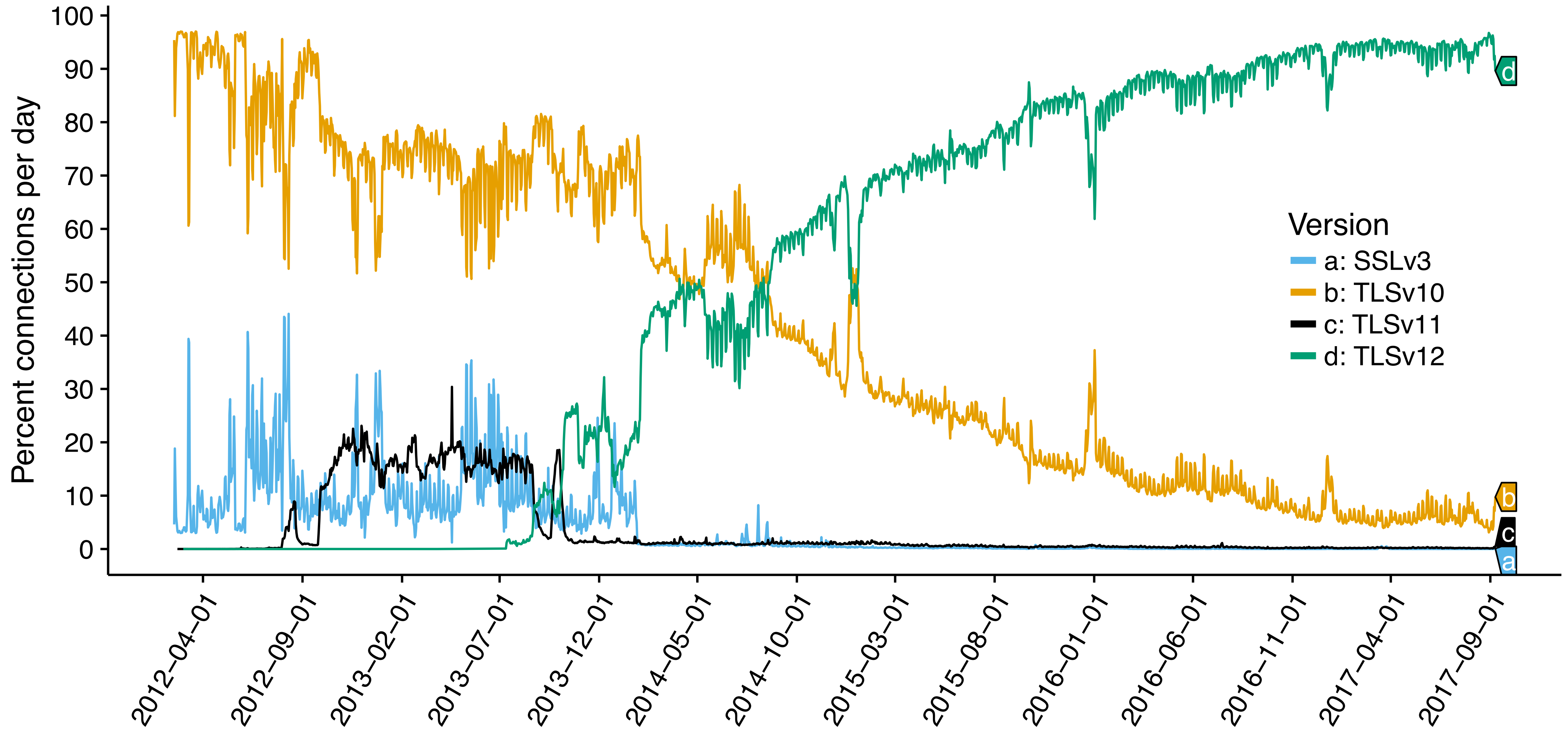
CT Precertificate SCTs:

..Random string goes here

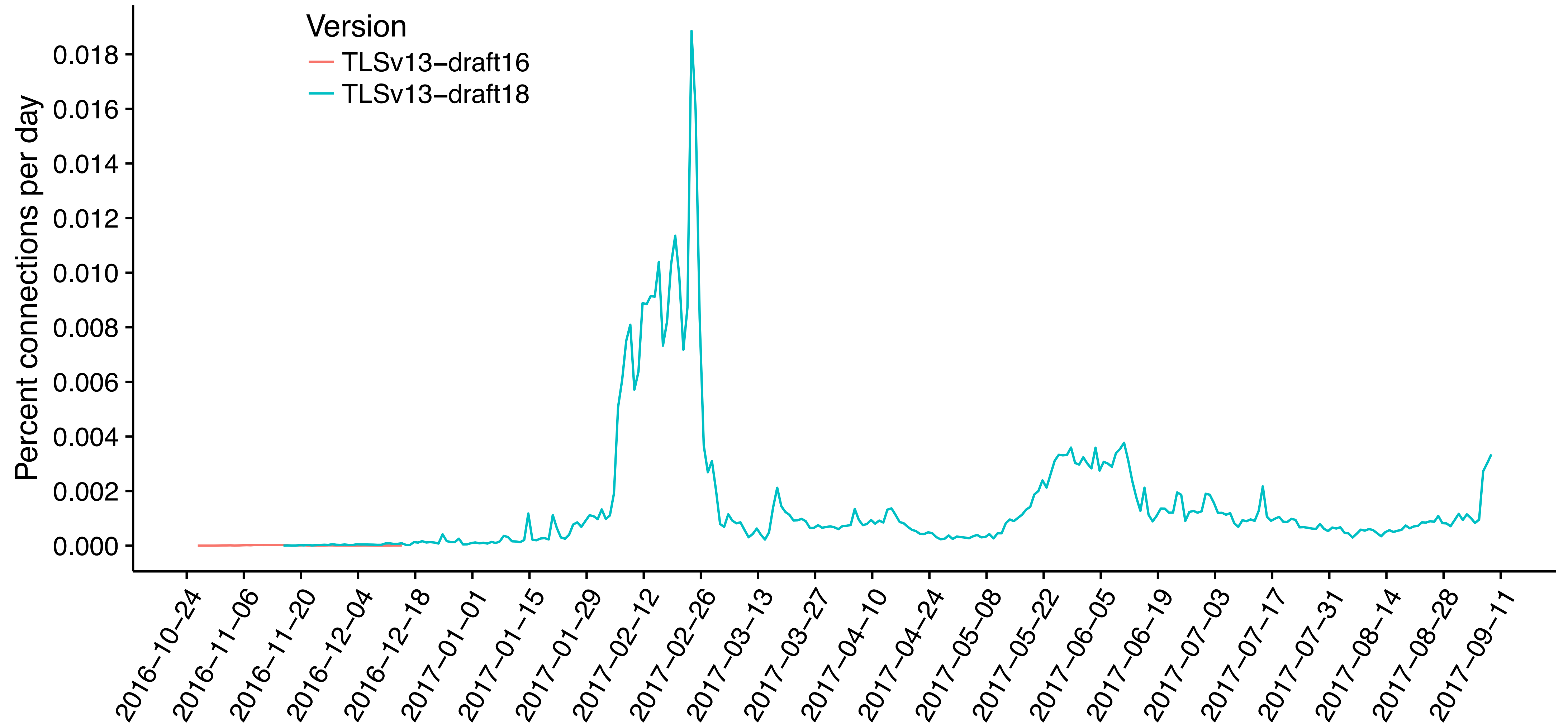
# Notary - Certificates



# TLS Version Evolution



# TLS Version Evolution



# HTTP/2

