SSL Research with Bro

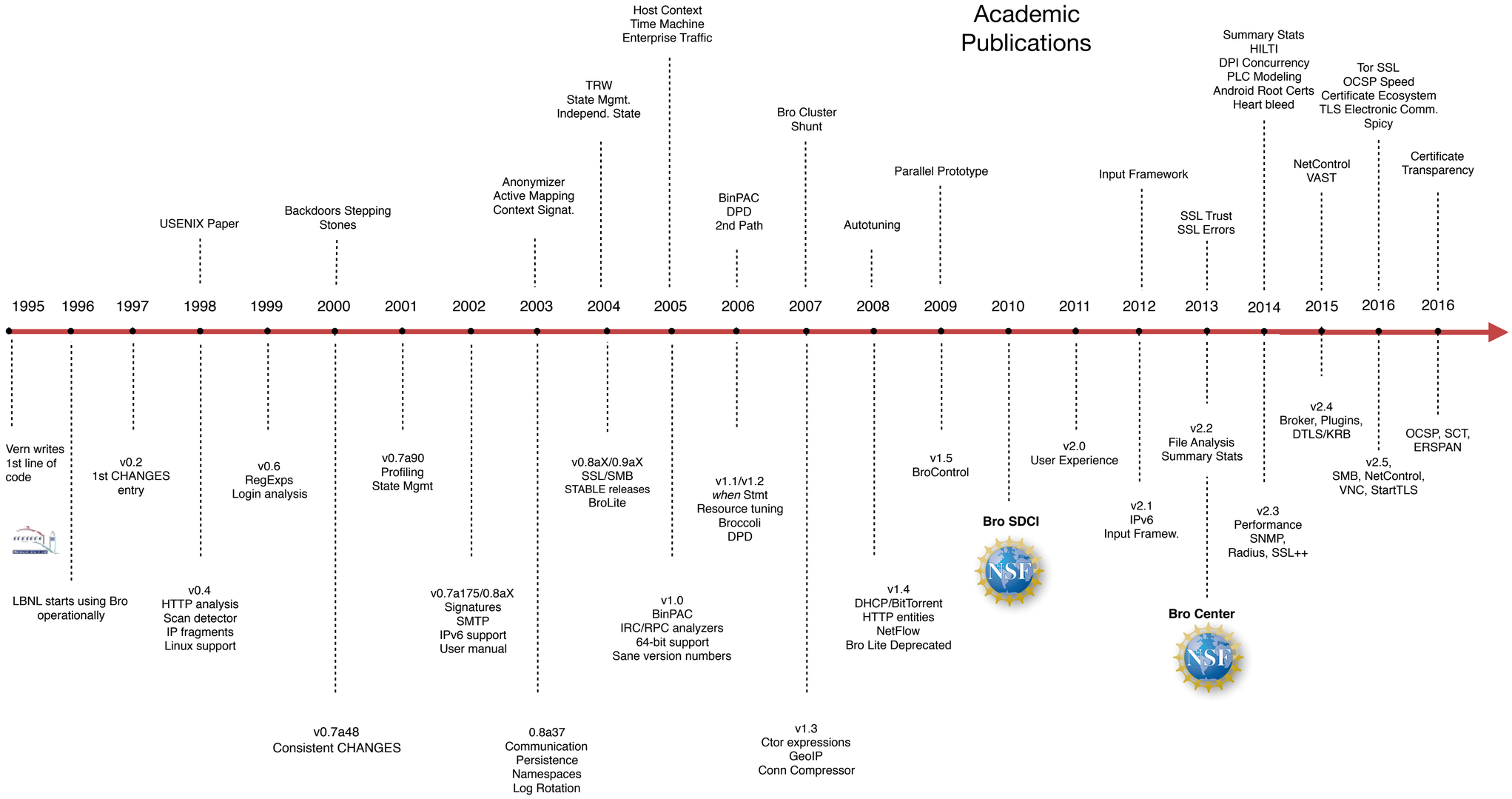
Johanna Amann

International Computer Science Institute

johanna@icir.org

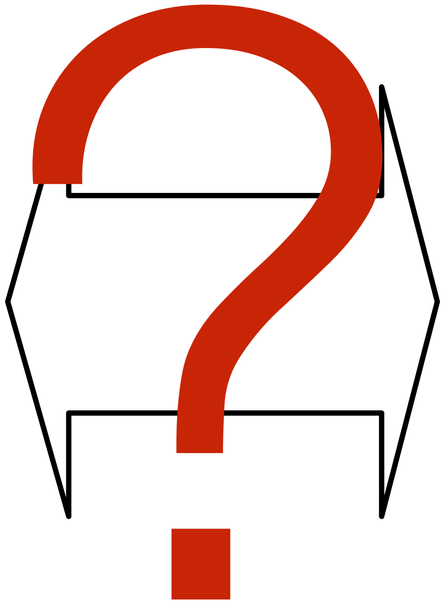
http://www.icir.org/johanna

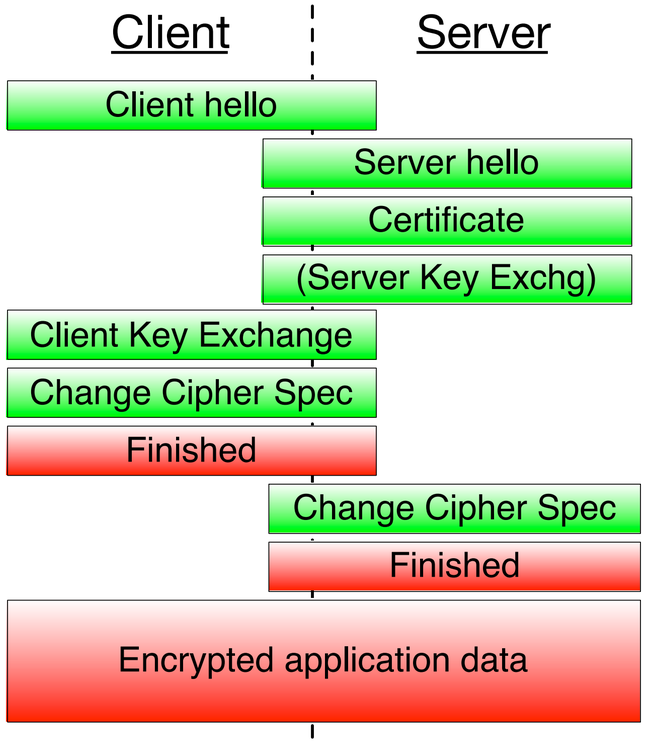
Bro History


Academic Publications
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2016
Vern writes 1st line of code
LBNL starts using Bro operationally
v0.2 1st CHANGES entry
v0.4 HTTP analysis Scan detector IP fragments Linux support
USENIX Paper
v0.6 RegExps Login analysis
Backdoors Stepping Stones
v0.7a48 Consistent CHANGES
v0.7a90 Profiling State Mgmt
v0.7a175/0.8aX Signatures SMTP IPv6 support User manual
Anonymizer Active Mapping Context Signat.
0.8a37 Communication Persistence Namespaces Log Rotation
TRW State Mgmt. Independ. State
v0.8aX/0.9aX SSL/SMB STABLE releases BroLite
Host Context Time Machine Enterprise Traffic
v1.0 BinPAC IRC/RPC analyzers 64-bit support Sane version numbers
BinPAC DPD 2nd Path
v1.1/v1.2 when Stmt Resource tuning Broccoli DPD
Bro Cluster Shunt
v1.3 Ctor expressions GeoIP Conn Compressor
Autotuning
v1.4 DHCP/BitTorrent HTTP entities NetFlow Bro Lite Deprecated
Parallel Prototype
v1.5 BroControl
Bro SDCI
NSF
v2.0 User Experience
Input Framework
v2.1 IPv6 Input Framew.
SSL Trust SSL Errors
v2.2 File Analysis Summary Stats
Bro Center
NSF
Summary Stats HILTI DPI Concurrency PLC Modeling Android Root Certs Heart bleed
v2.3 Performance SNMP, Radius, SSL++
NetControl VAST
v2.4 Broker, Plugins, DTLS/KRB
Tor SSL OCSP Speed Certificate Ecosystem TLS Electronic Comm. Spicy
v2.5, SMB, NetControl, VNC, StartTLS
Certificate Transparency
OCSP, SCT, ERSPAN

Bro SSL - v1.5.3

- ssl_certificate_seen
- ssl_certificate
- ssl_conn_attempt
- ssl_conn_alert
- ssl_conn_server_reply
- ssl_conn_weak
- ssl_conn_established
- ssl_session_insertion
- ssl_conn_reused
- process_X509_extensions
- ssl_X509_error





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

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_server_curve

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_change_cipher_spec

x509_extension

x509_ext_basic_constraints

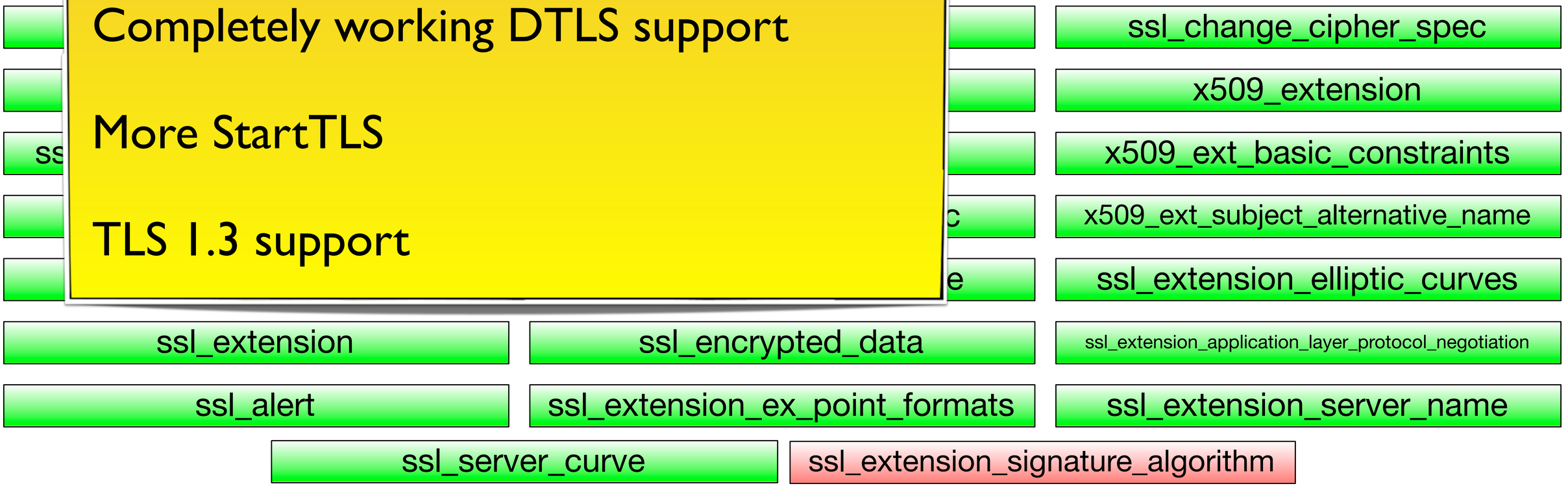
x509_ext_subject_alternative_name

ssl_extension_elliptic_curves

ssl_extension_application_layer_protocol_negotiation

ssl_extension_server_name

Bro SSL Events - v2.5



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_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_server_curve

ssl_extension_signature_algorithm

Bro SSL Events - master

client_hello	ssl_stapled_ocsp	ssl_change_cipher_spec
server_hello	ssl_encrypted_data	x509_extension
ssl_session_ticket_handshake	ssl_dh_server_params	x509_ext_basic_constraints
ssl_established	ssl_change_cipher_spec	x509_ext_subject_alternative_name
x509_certificate	ssl_handshake_message	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	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

Bro SSL Events - master

client_hello	ssl_stapled_ocsp	ssl_change_cipher_spec
server_hello	ssl_encrypted_data	x509_extension
	ams	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

OCSP support

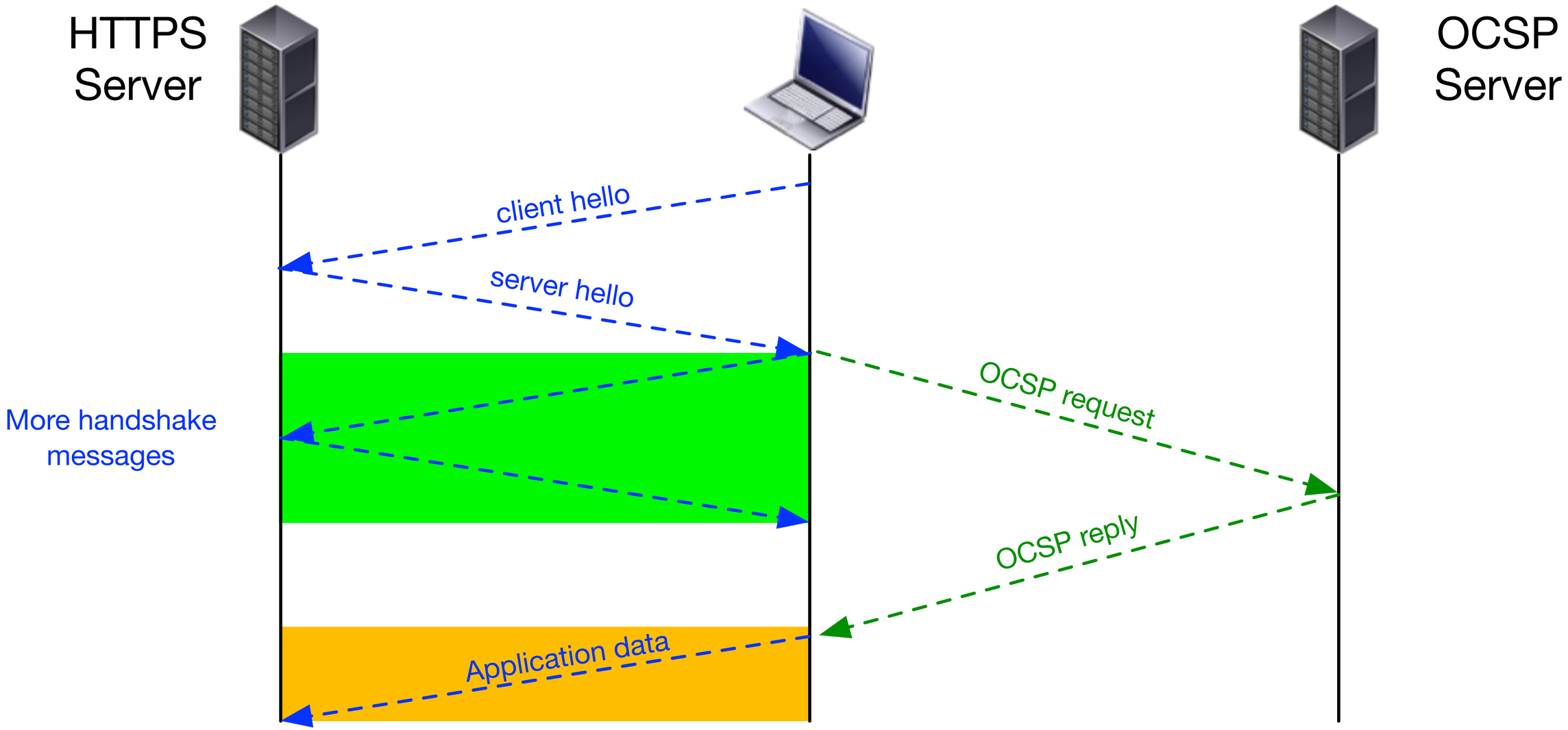
SCT Support (Certificate Transparency)

TLS 1.3 extensions

TLS 1.3

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

OCSP



Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

@load files/x509/log-ocsp

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

Certificate Transparency

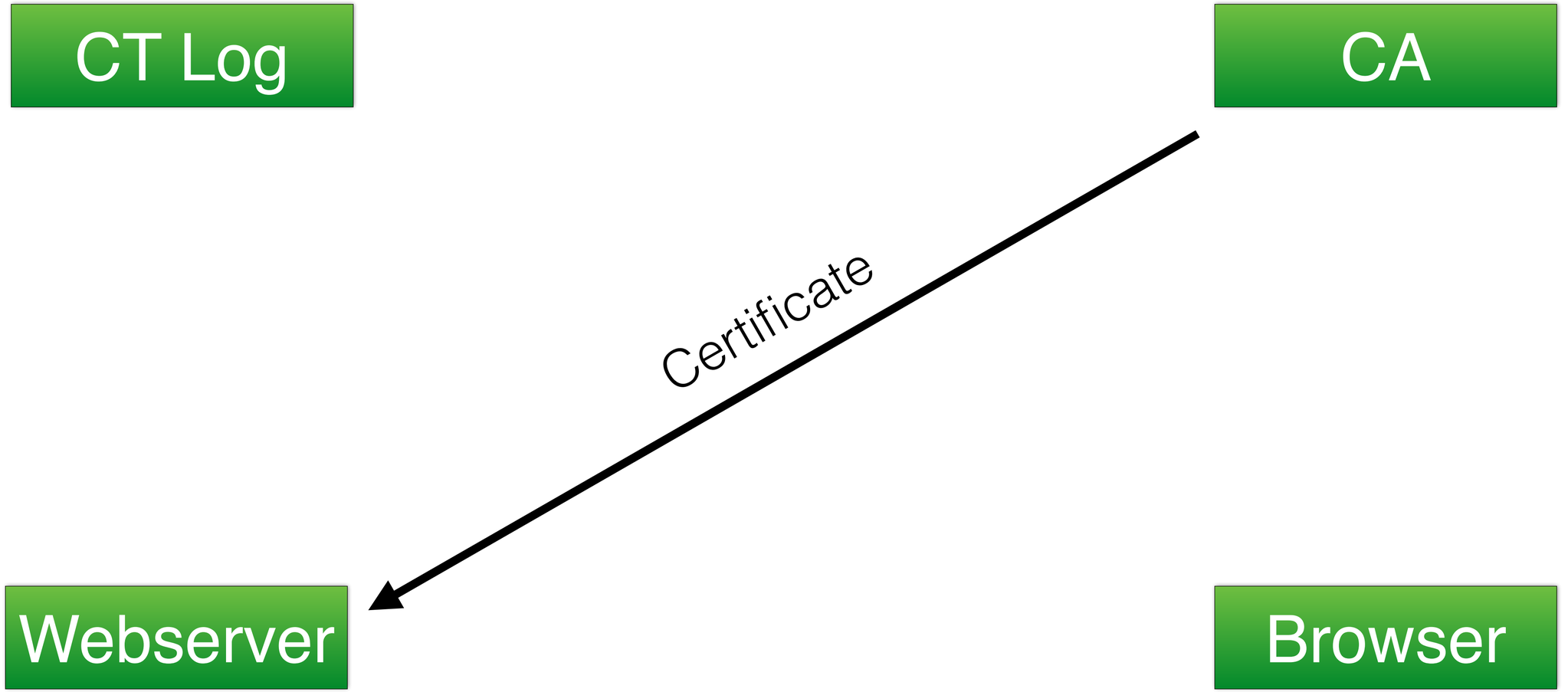
CT Log

CA

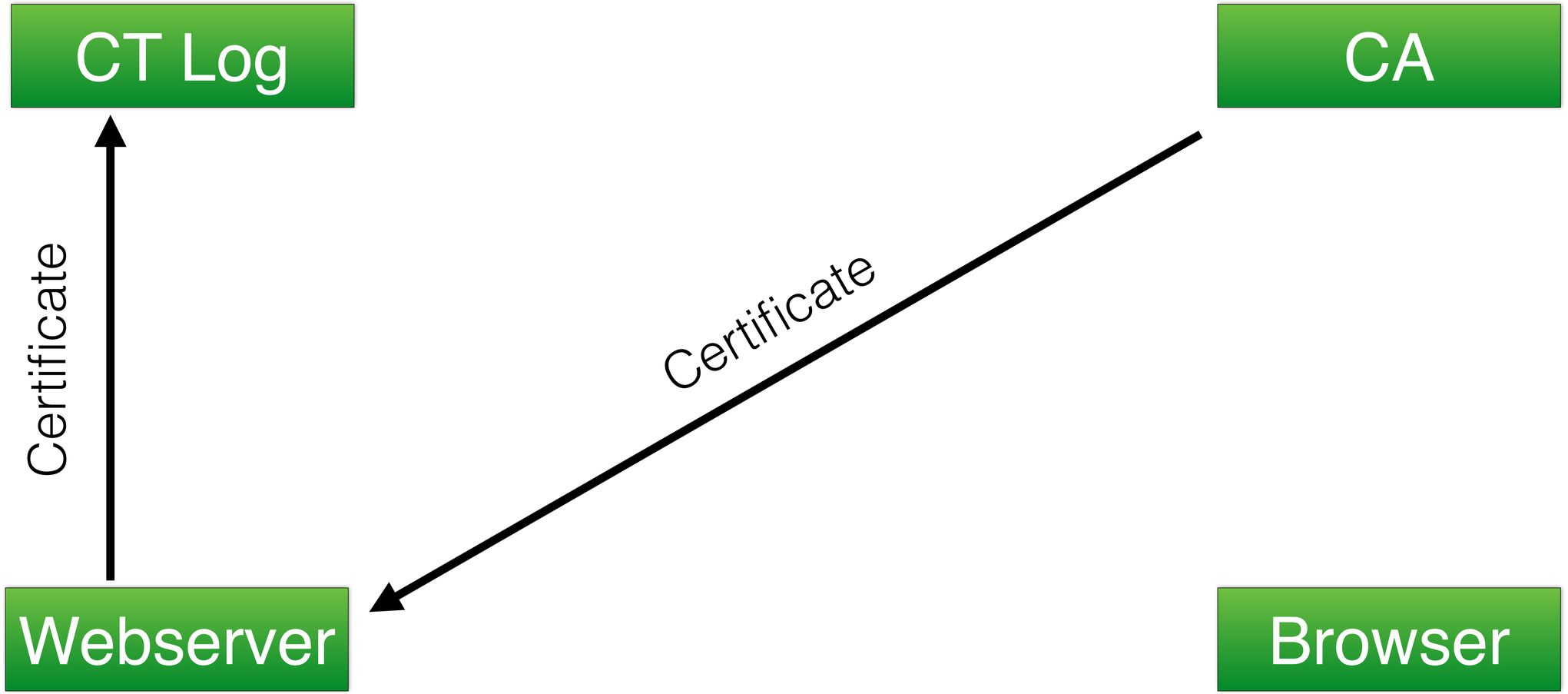
Webserver

Browser

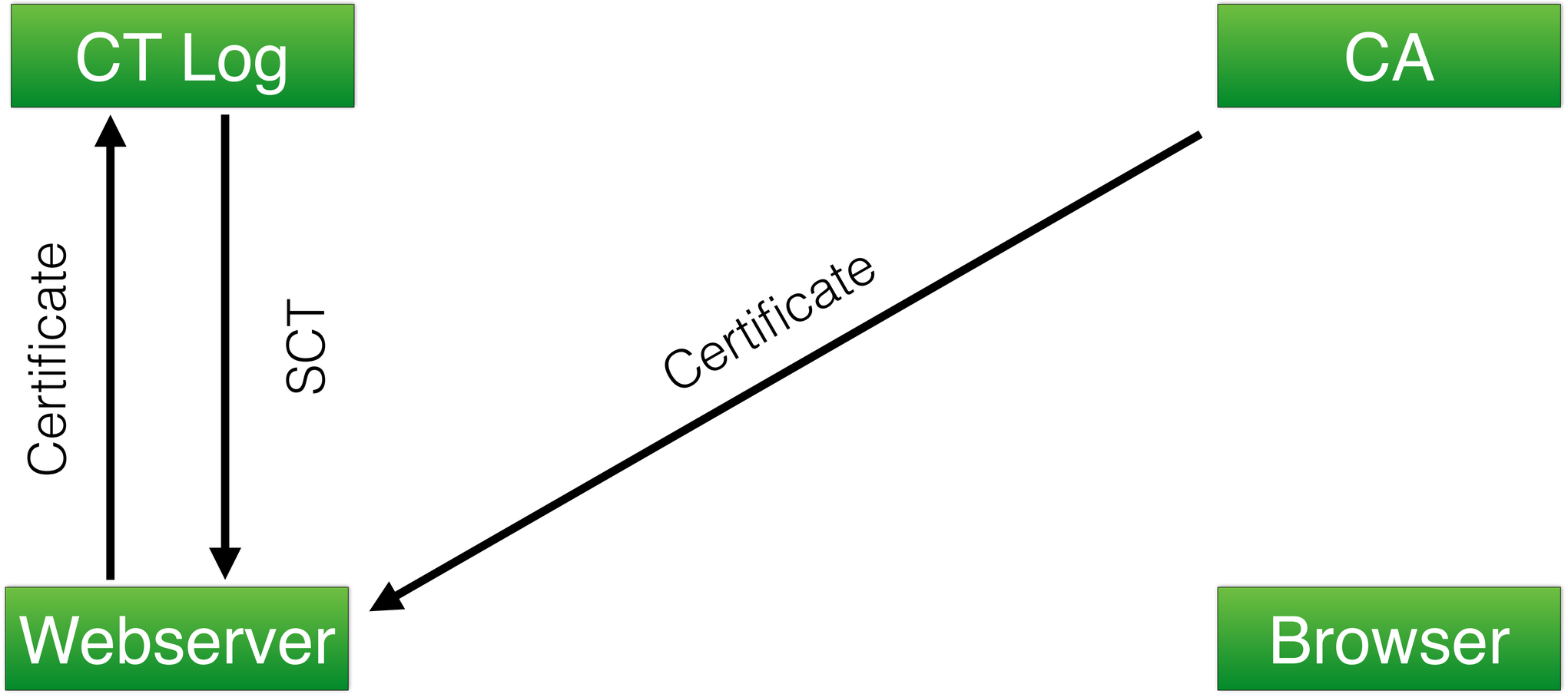
Certificate Transparency



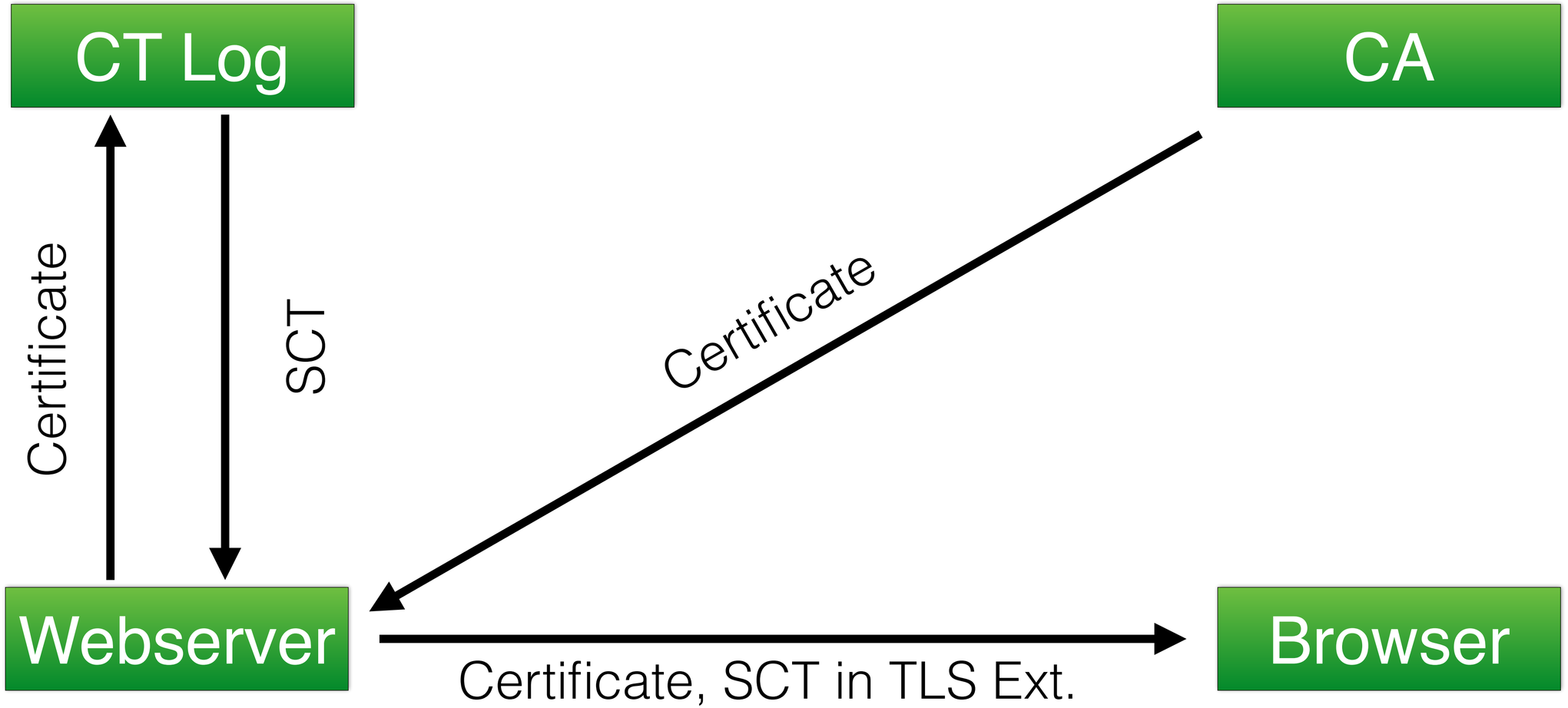
Certificate Transparency



Certificate Transparency



Certificate Transparency



Certificate Transparency

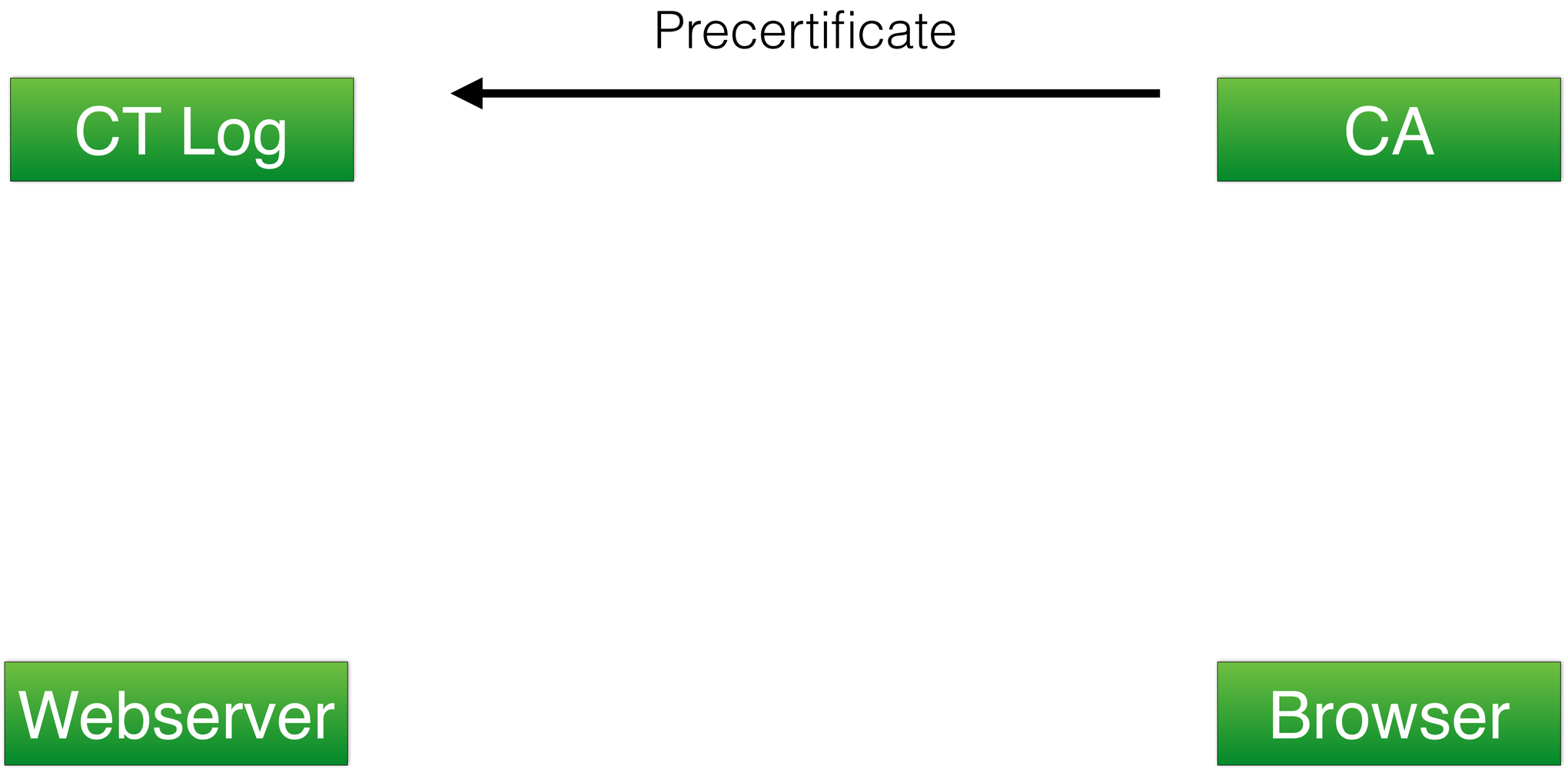
CT Log

CA

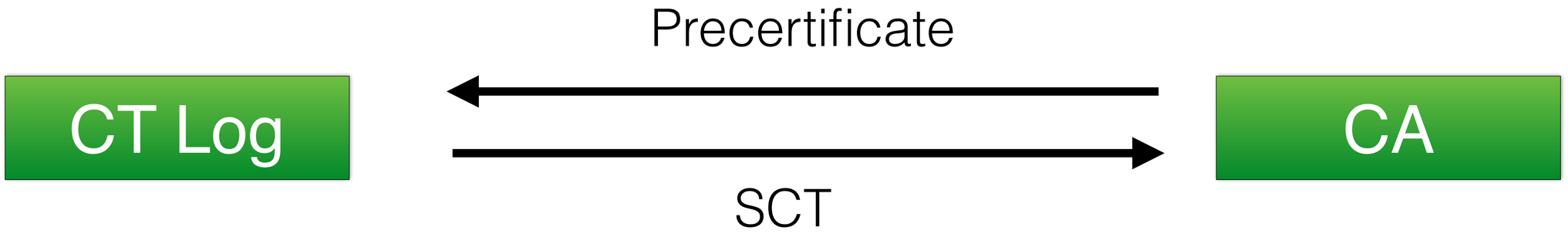
Webserver

Browser

Certificate Transparency



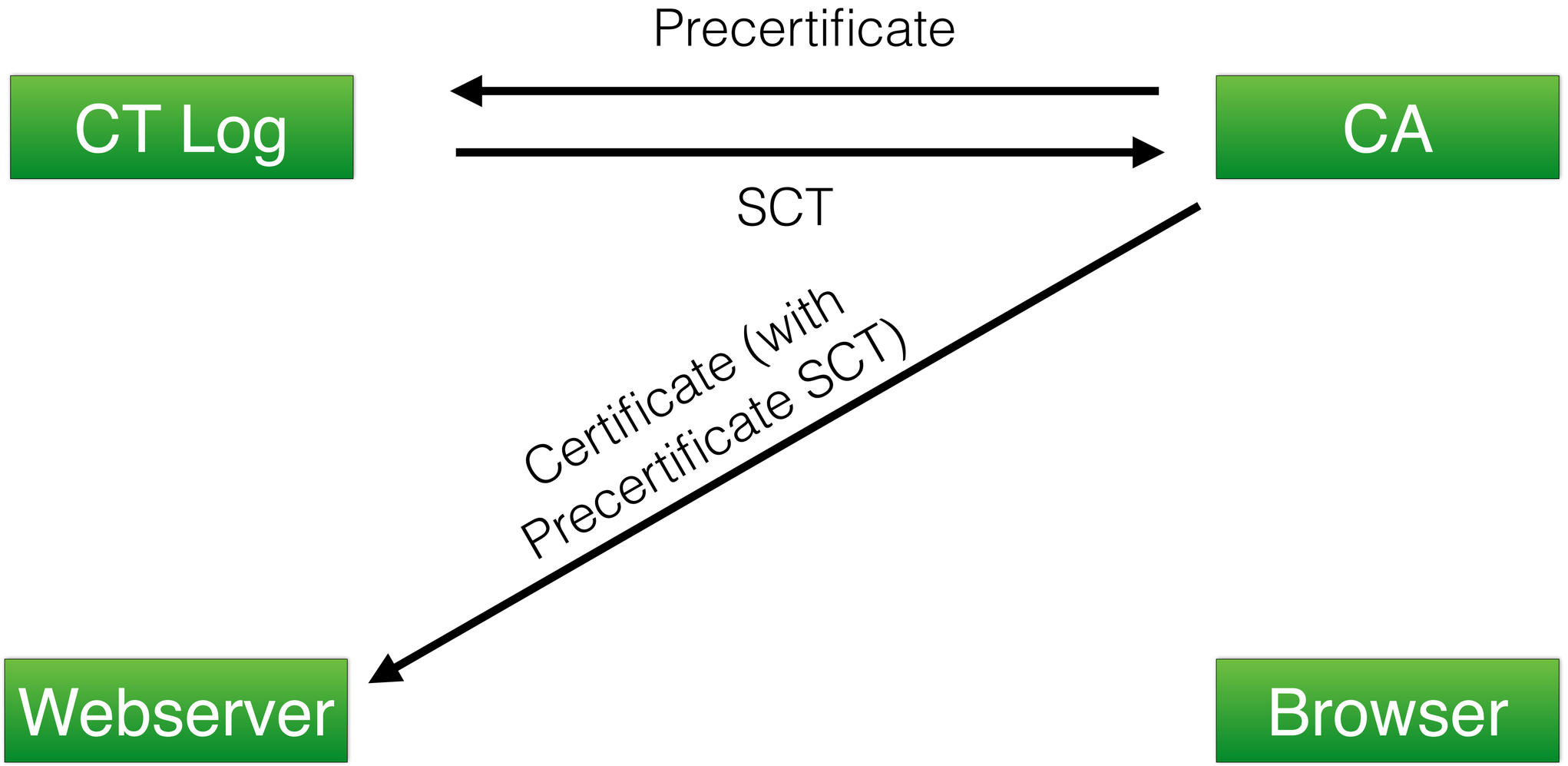
Certificate Transparency



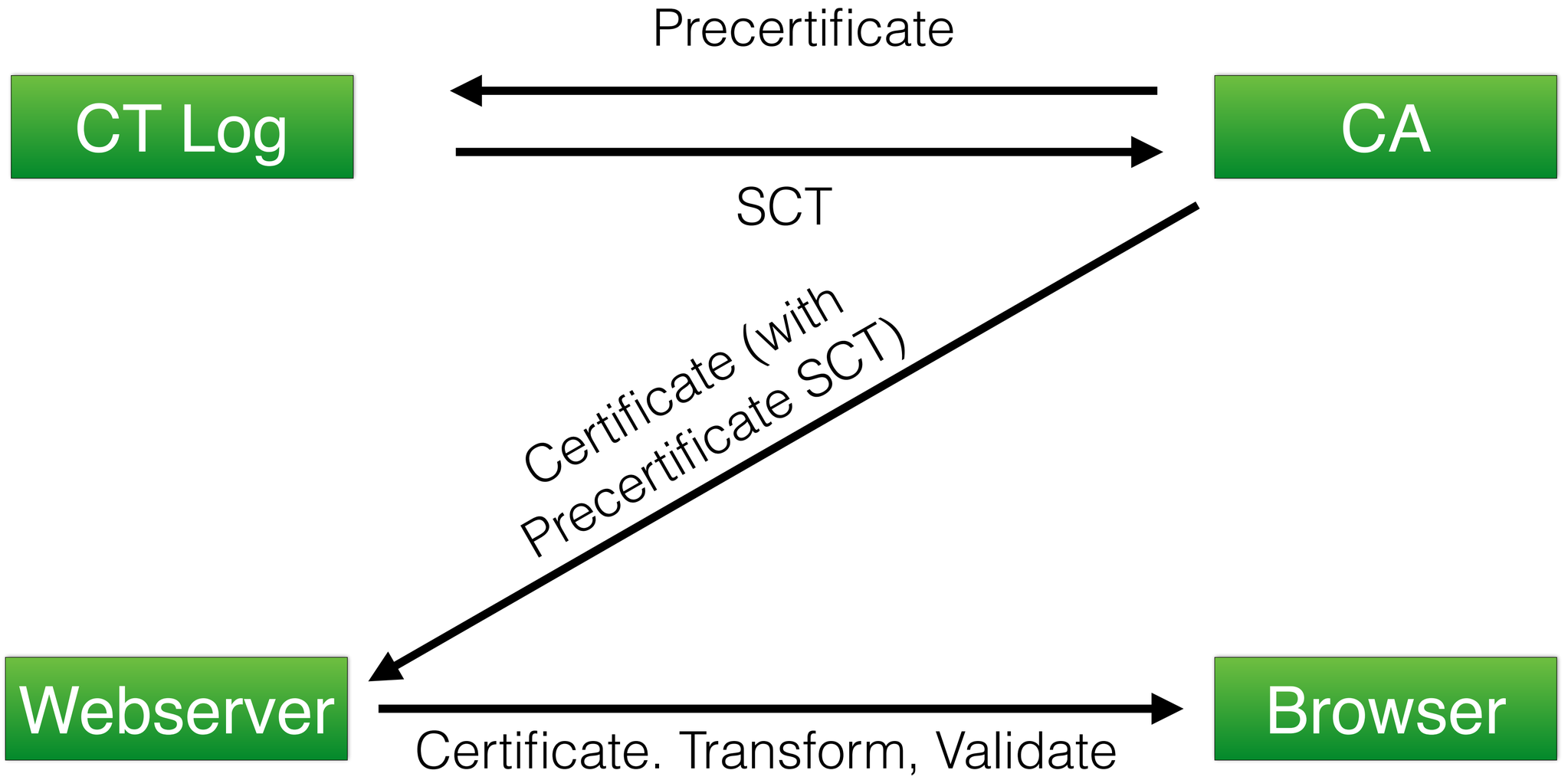
Webserver

Browser

Certificate Transparency



Certificate Transparency



Certificate Transparency

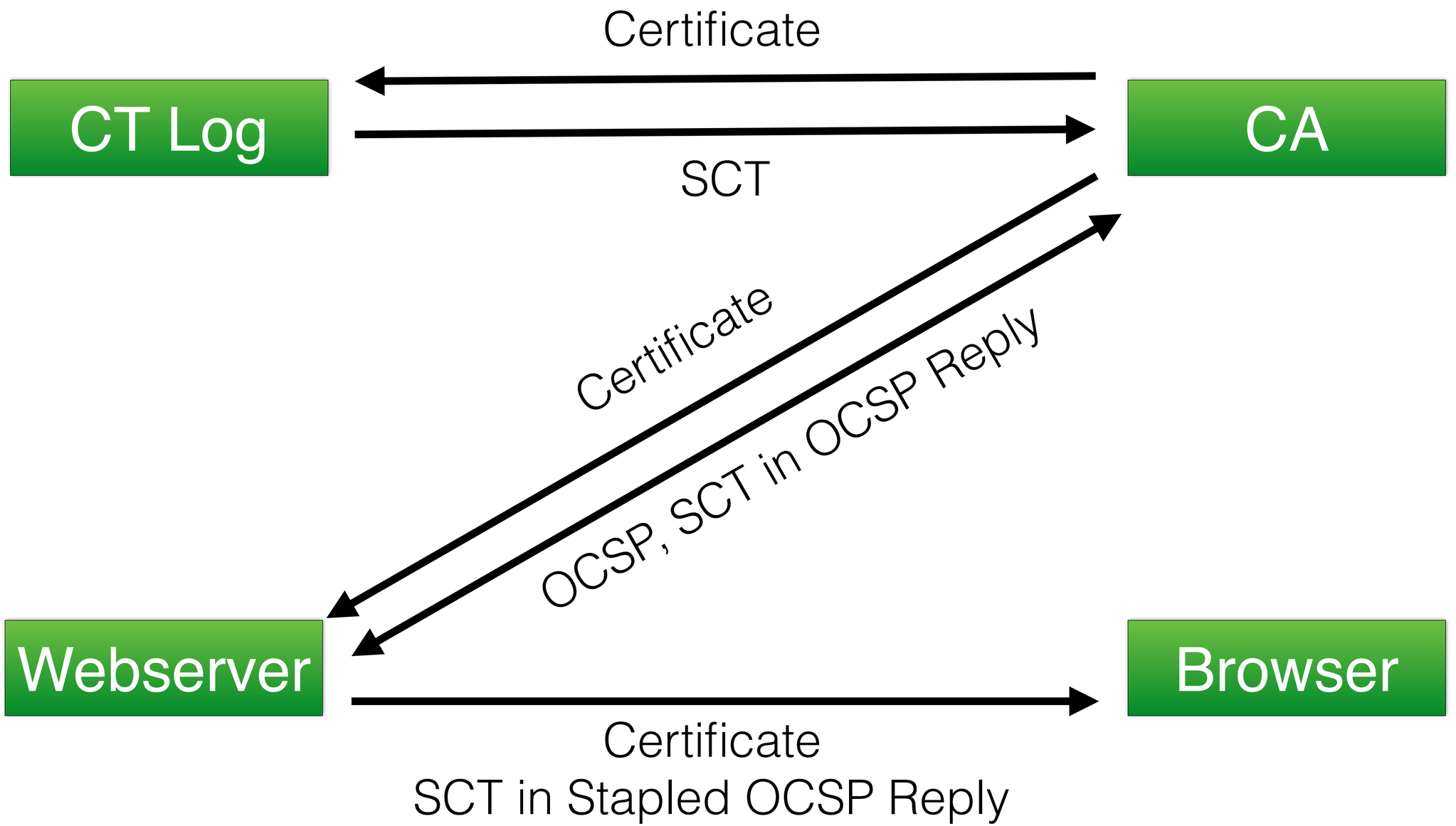
CT Log

CA

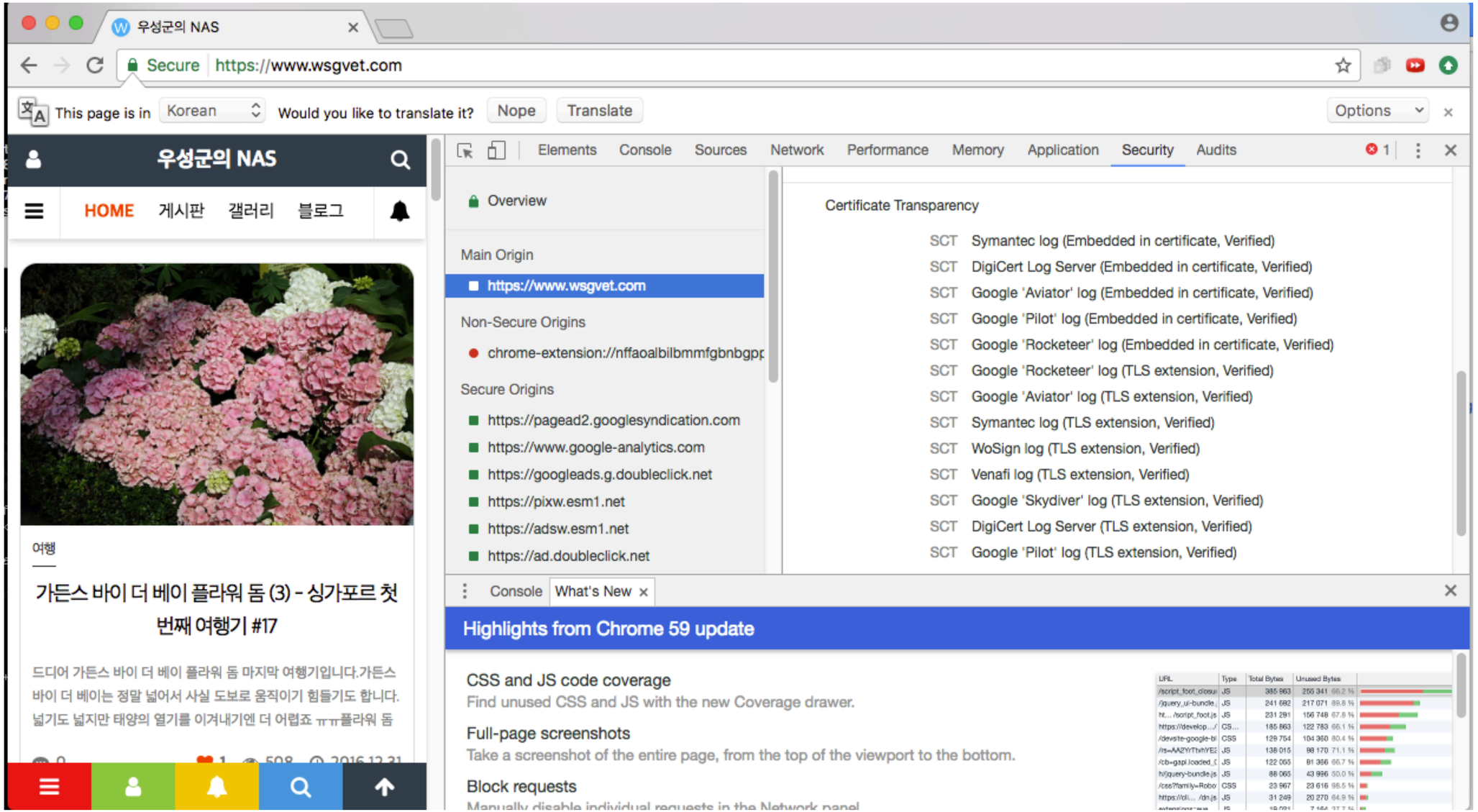
Webserver

Browser

Certificate Transparency

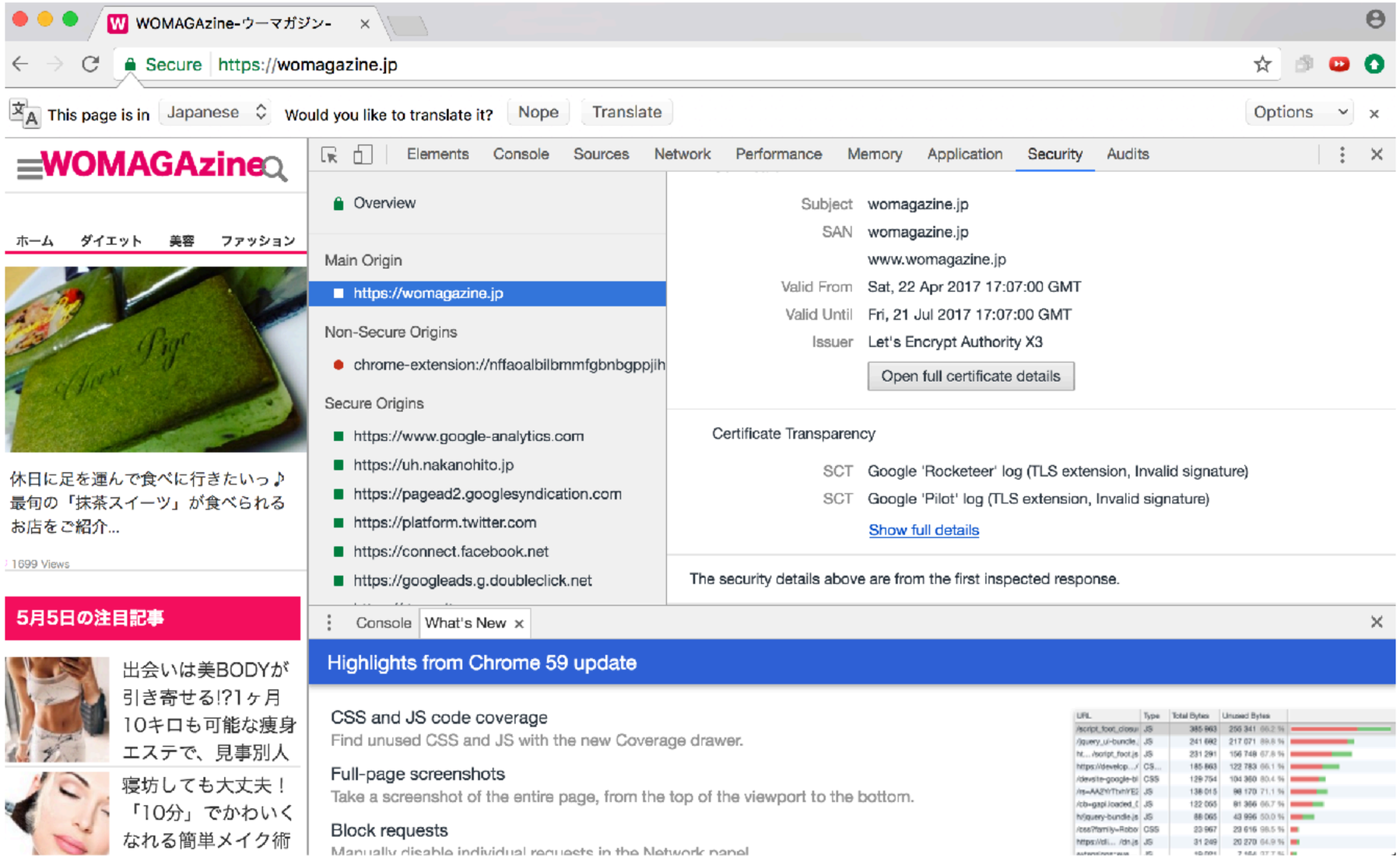


TLS Versions



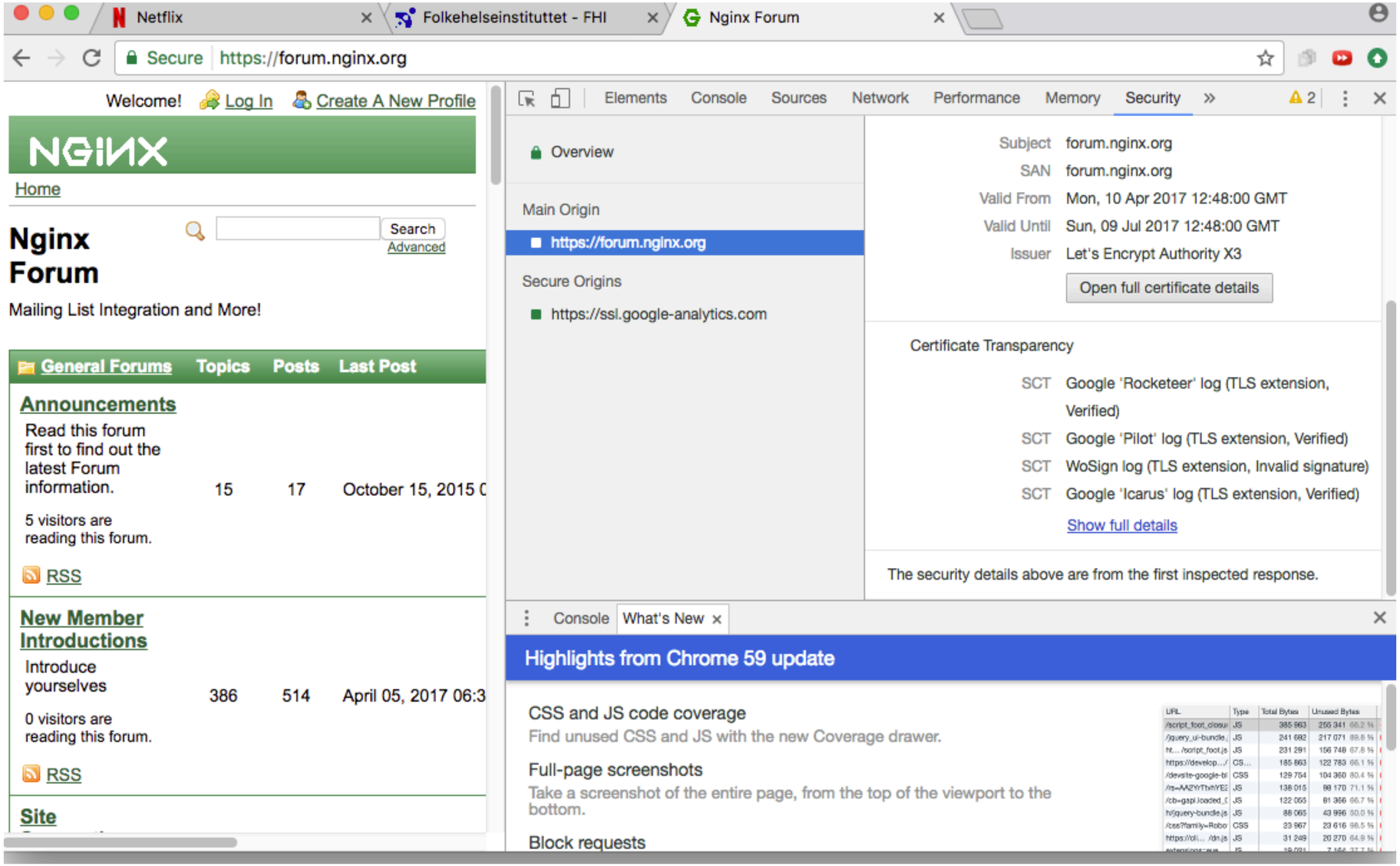
Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

TLS Versions



Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

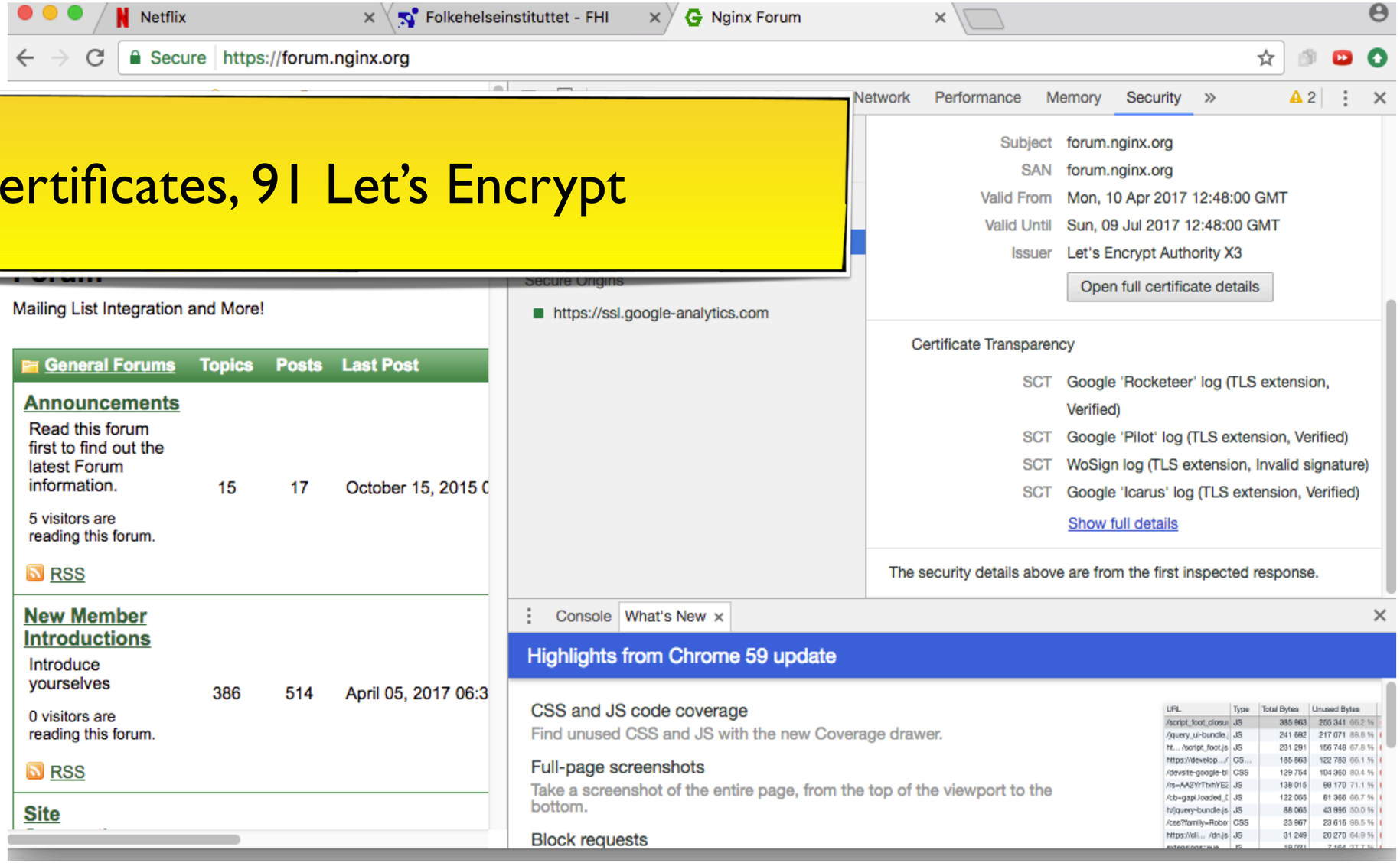
TLS Versions



Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

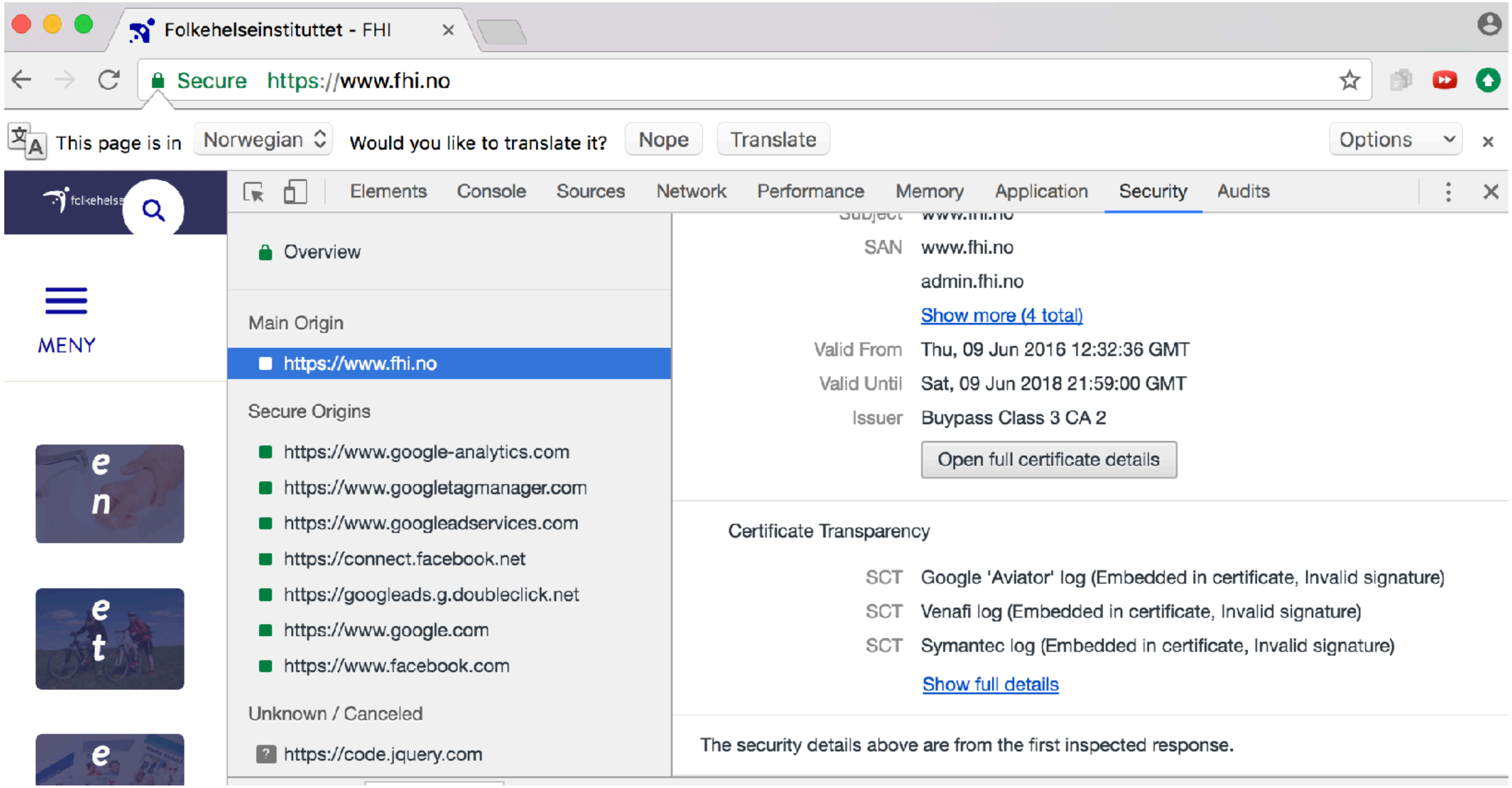
TLS Versions

105 Certificates, 91 Let's Encrypt



Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

TLS Versions



Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

@load protocols/ssl/validate-sct.bro

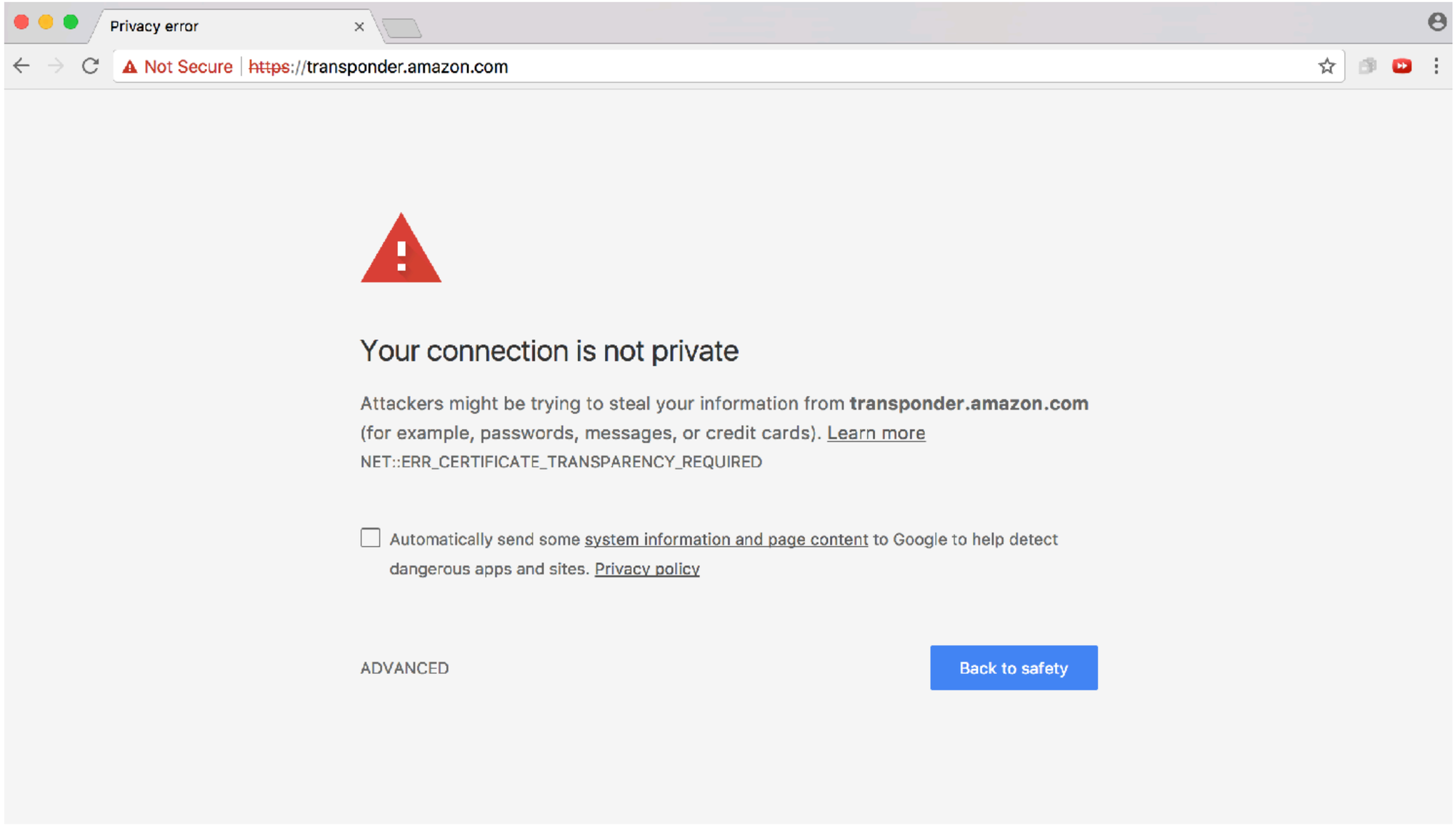
ts	1484228945.191472
id.resp_h	97.107.139.108
version	TLSv12
cipher	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
curve	secp256r1
server_name	ritter.vg
subject	CN=ritter.vg,OU=PositiveSSL,OU=Domain…
issuer	CN=COMODO RSA Domain Validation Secure…
validation_status	ok
valid_ct_logs	3
valid_ct_operators	1

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%)

Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

Log Operators



Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

SCT Statistics

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

Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

```
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
```

Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

```
 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]:3049301F06082B06010505073001861368747470 3A2F2F73732E73796D63642E636F6D30260
D63622E636F6D2F73732E637274
 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
```

Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

```
 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]:3049301F06082B06010505073001861368747470 3A2F2F73732E73796D63642E636F6D30260
D63622E636F6D2F73732E637274
 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
```

Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

Normal SCT

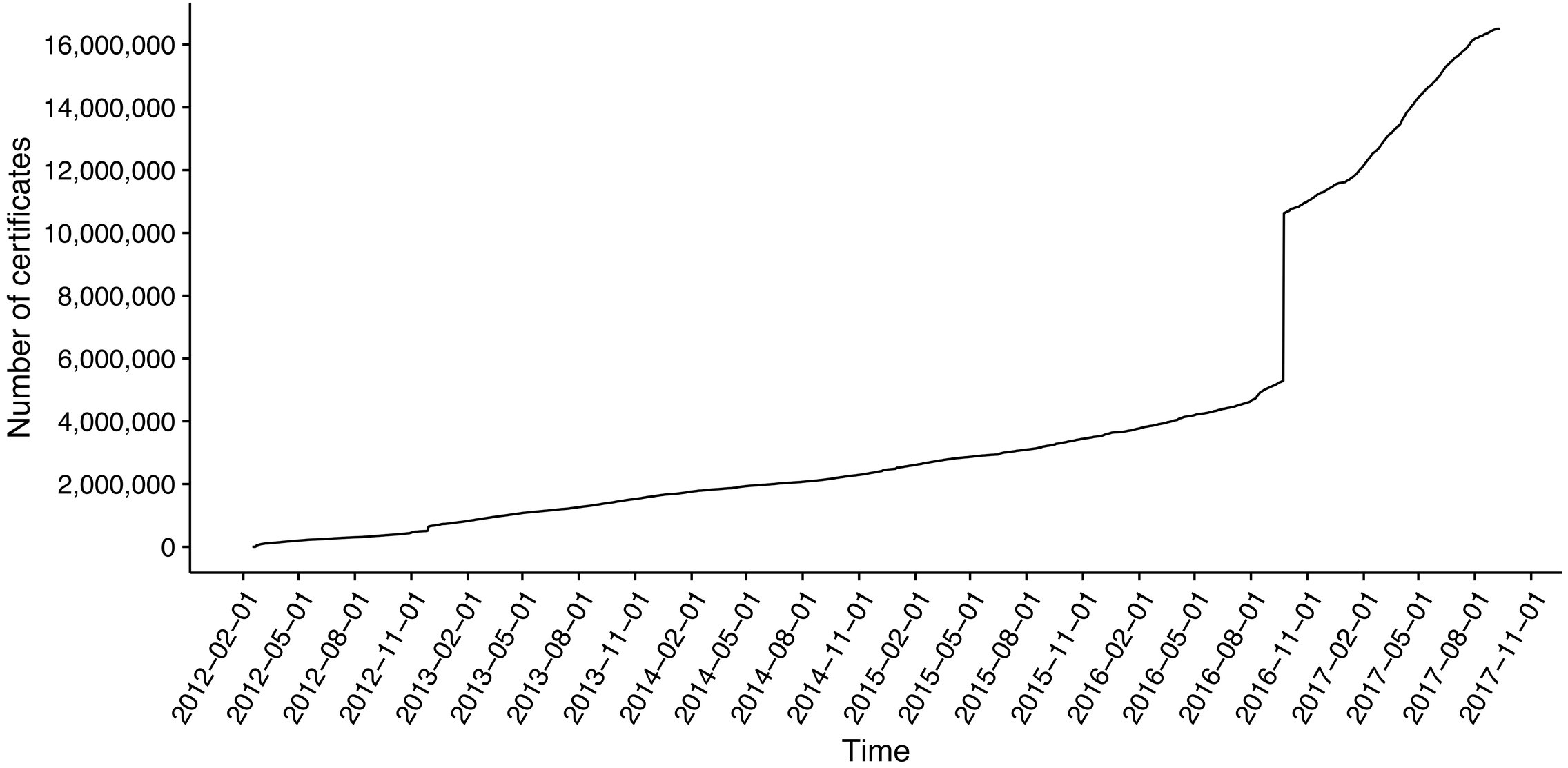
```
CT Precertificate SCTs:
    Signed Certificate Timestamp:
        Version   : v1(0)
        Log ID    : DD:EB:1D:2B:7A:0D:4F:A6:20:8B:81:AD:81:68:70:7E:
                    2E:8E:9D:01:D5:5C:88:8D:3D:11:C4:CD:B6:EC:BE:CC
        Timestamp : Aug 17 17:25:11.747 2016 GMT
        Extensions: none
        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
```

Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

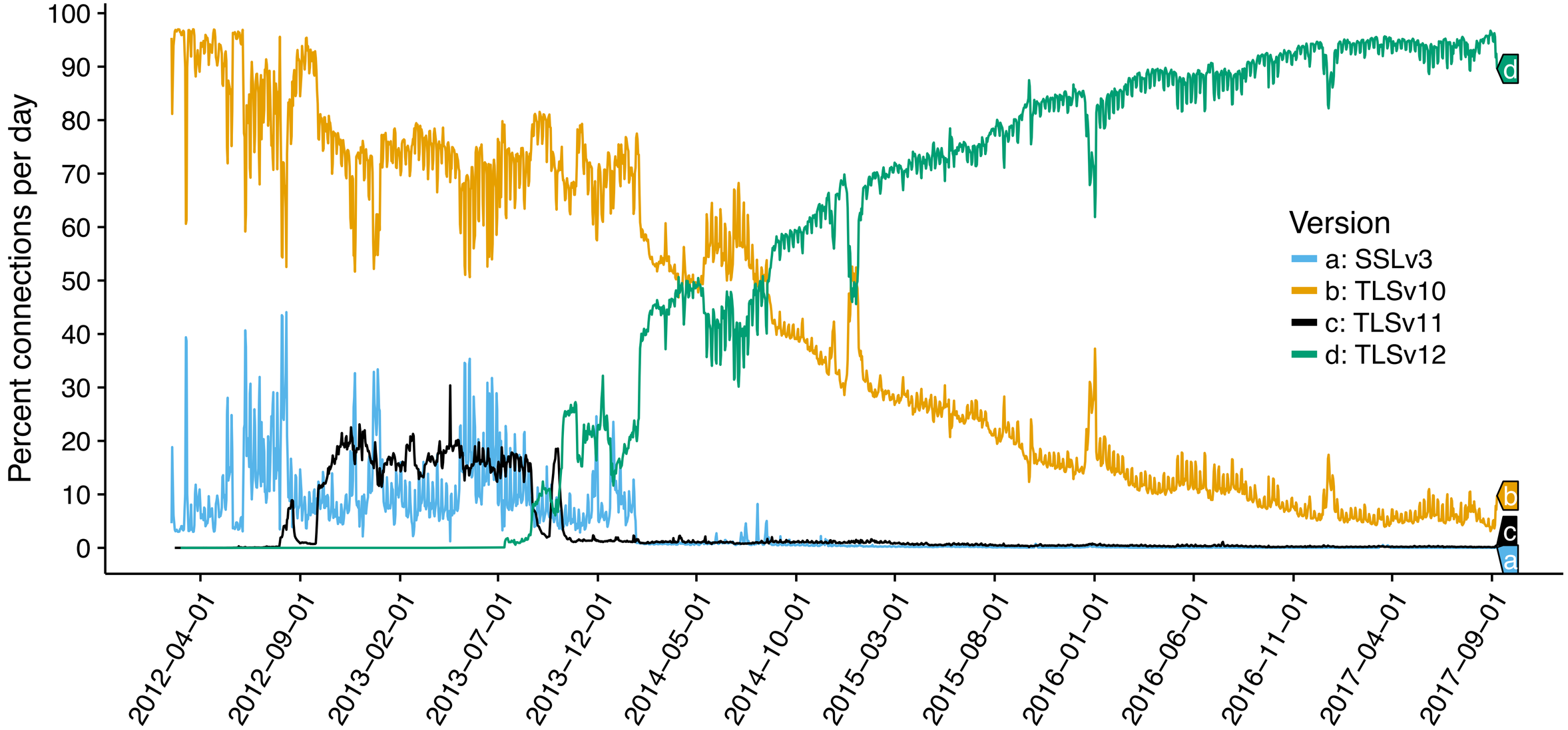
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            36:9a:c7:3d:67:06:3a:a2:75:83:0d:fc:66:84:1c:1e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
        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
```

Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

Notary - Certificates

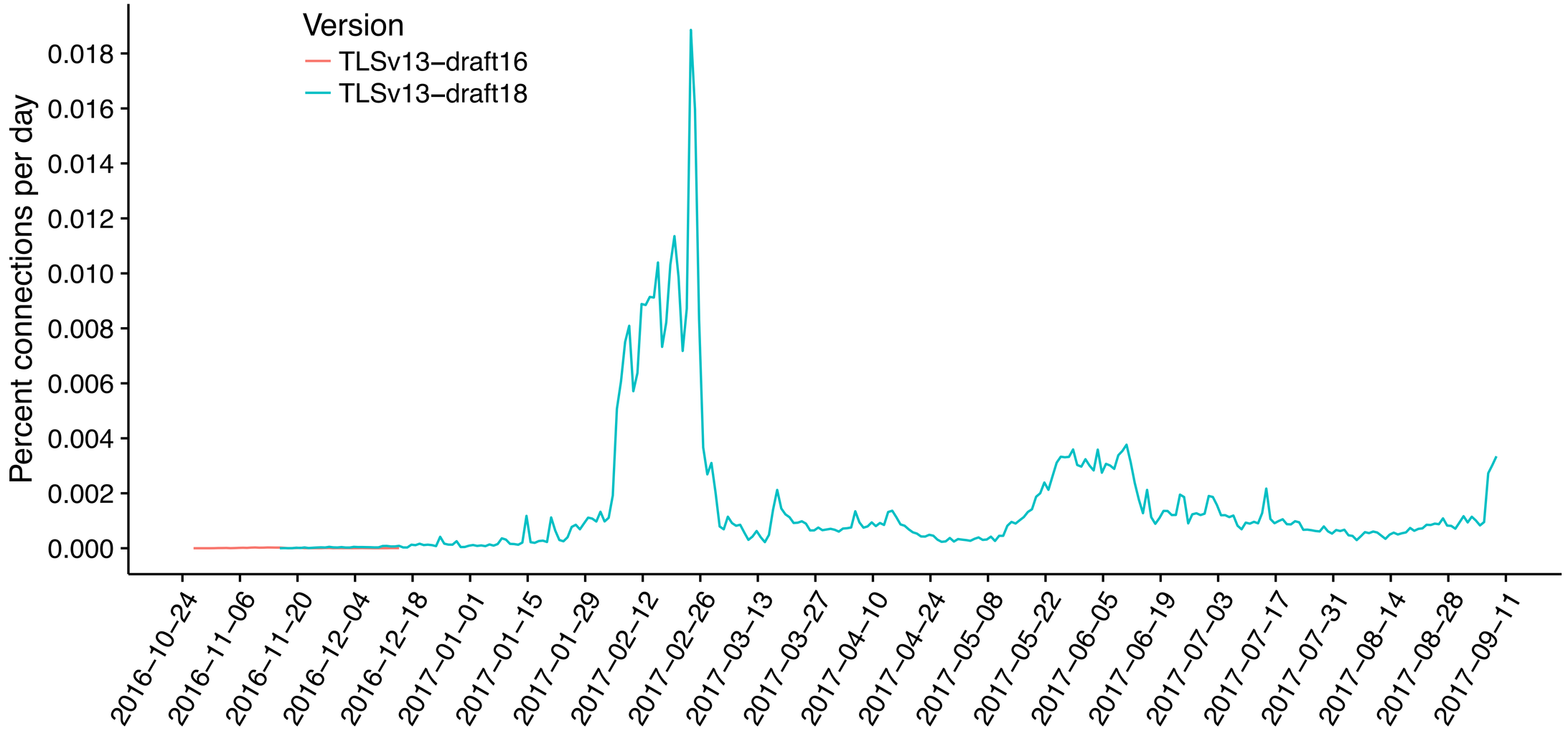


TLS Version Evolution

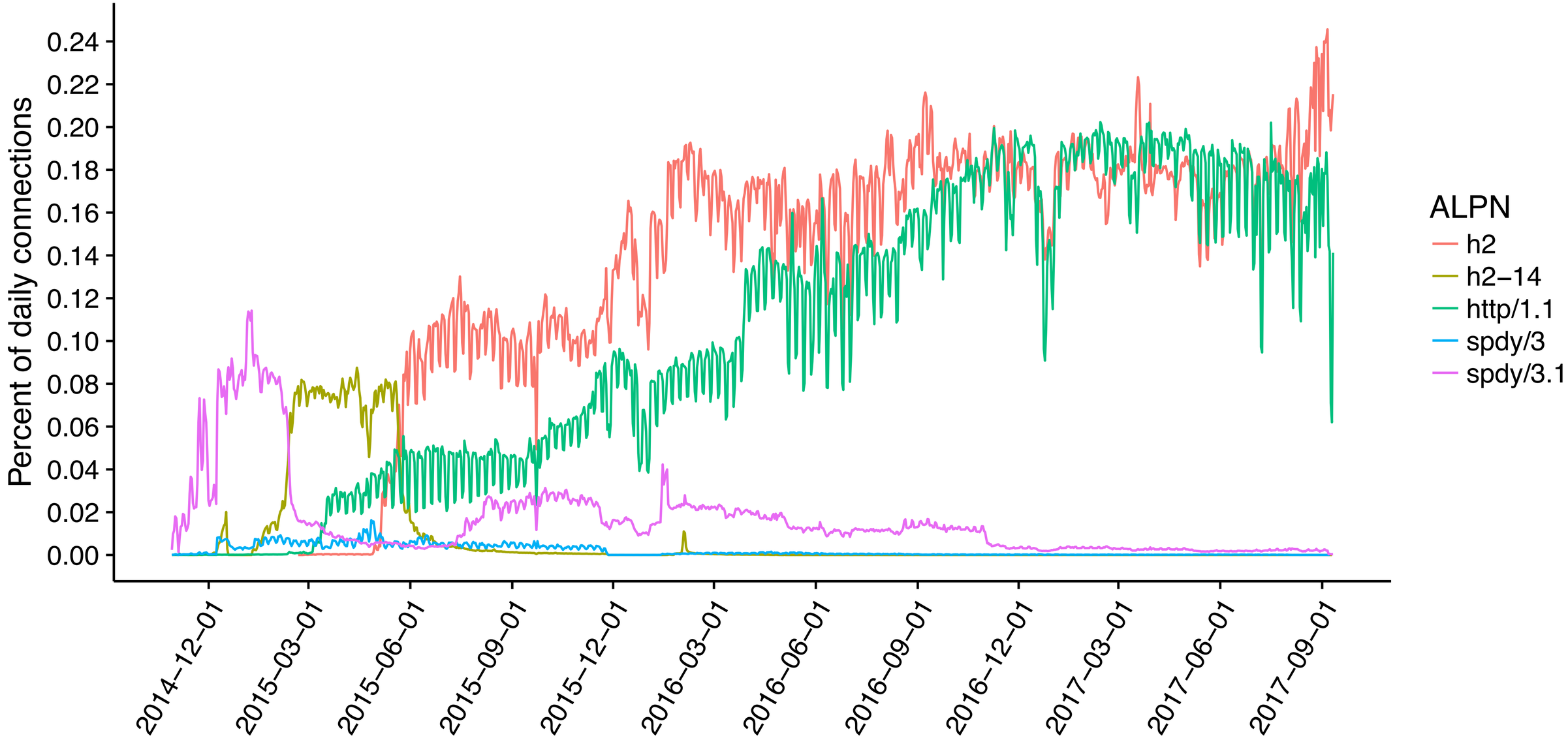


Mission Accomplished? HTTPS Security after DigiNotar
J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, IMC 2017

TLS Version Evolution



HTTP/2


Percent of daily connections
0.24
0.22
0.20
0.18
0.16
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.00
2014–12–01
2015–03–01
2015–06–01
2015–09–01
2015–12–01
2016–03–01
2016–06–01
2016–09–01
2016–12–01
2017–03–01
2017–06–01
2017–09–01
ALPN
h2
h2–14
http/1.1
spdy/3
spdy/3.1