Mission Accomplished? HTTPS Security after DigiNotar

Johanna Amann*	ICSI / LBL / Corelight
Oliver Gasser*	Technical University of Munich
Quirin Scheitle*	Technical University of Munich
Lexi Brent	The University of Sydney
Georg Carle	Technical University of Munich
Ralph Holz	The University of Sydney

* Joint First Authorship

TLS/HTTPS Security Extensions

- Certificate Transparency
- HSTS (HTTP Strict Transport Security)
- HPKP (HTTP Public Key Pinning)
- SCSV (TLS Fallback Signaling Cipher Suite Value)
- CAA (Certificate Authority Authorization)
- DANE-TLSA (DNS Based Authentication of Named Entities)

Methodology

- Active & passive scans
  - Shared pipeline where possible
- Active measurements from 2 continents
  - Largest Domain-based TLS scan so far
  - More than 192 Million domains
- Passive measurements on 3 continents
  - More than 2.4 Billion observed TLS connections

Certificate Transparency

CA

Issues Certificates

CT Log

Provides publicly auditable, append-only Log of certificates

Also provides proof of inclusion

Browser

Verifies proof of inclusion

Certificate Transparency

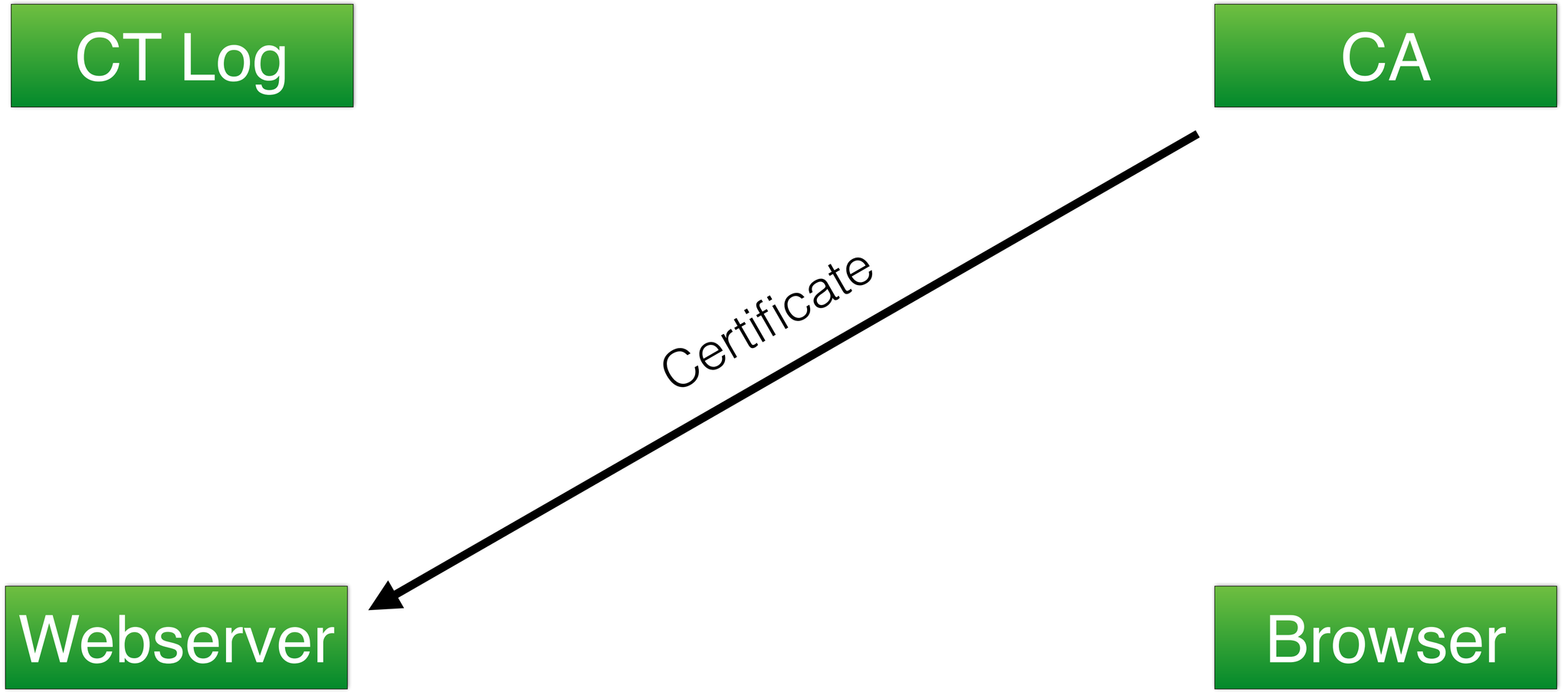
CT Log

CA

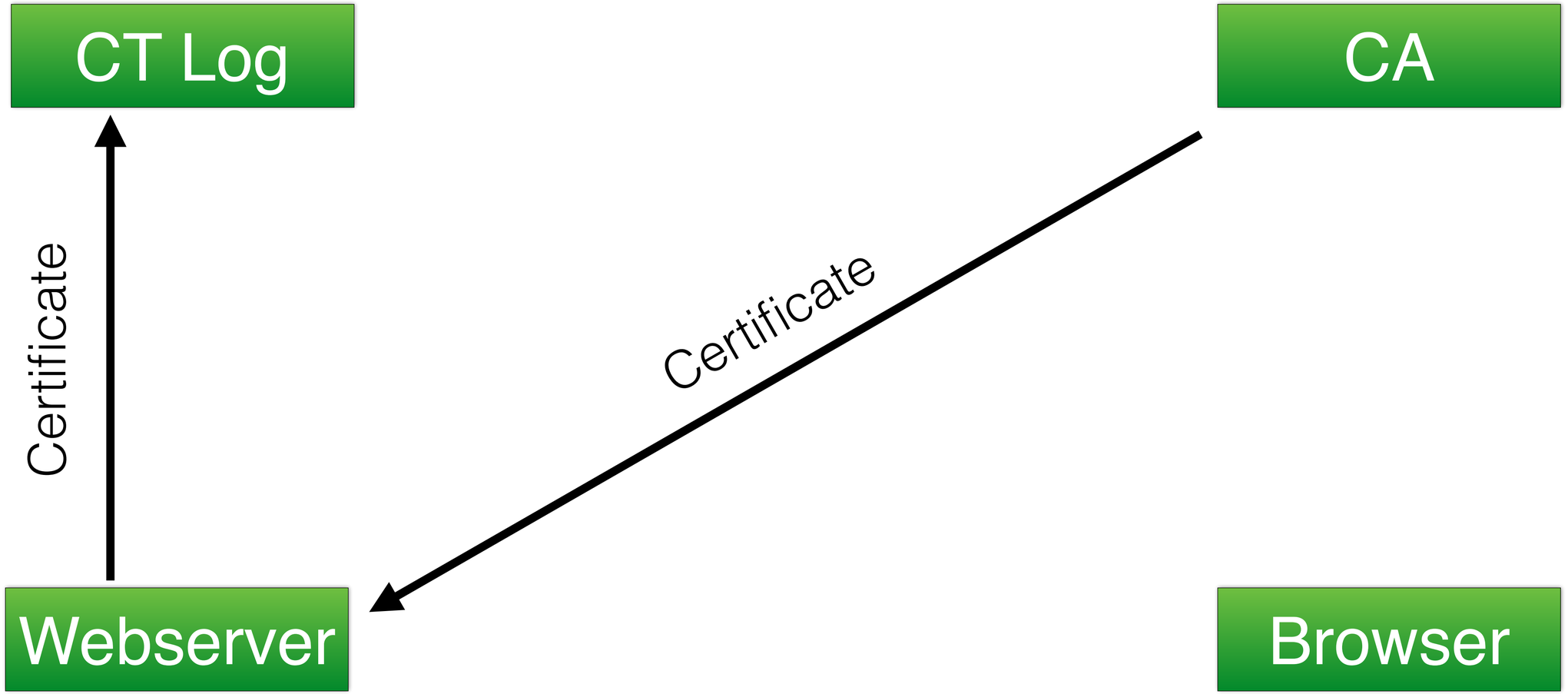
Webserver

Browser

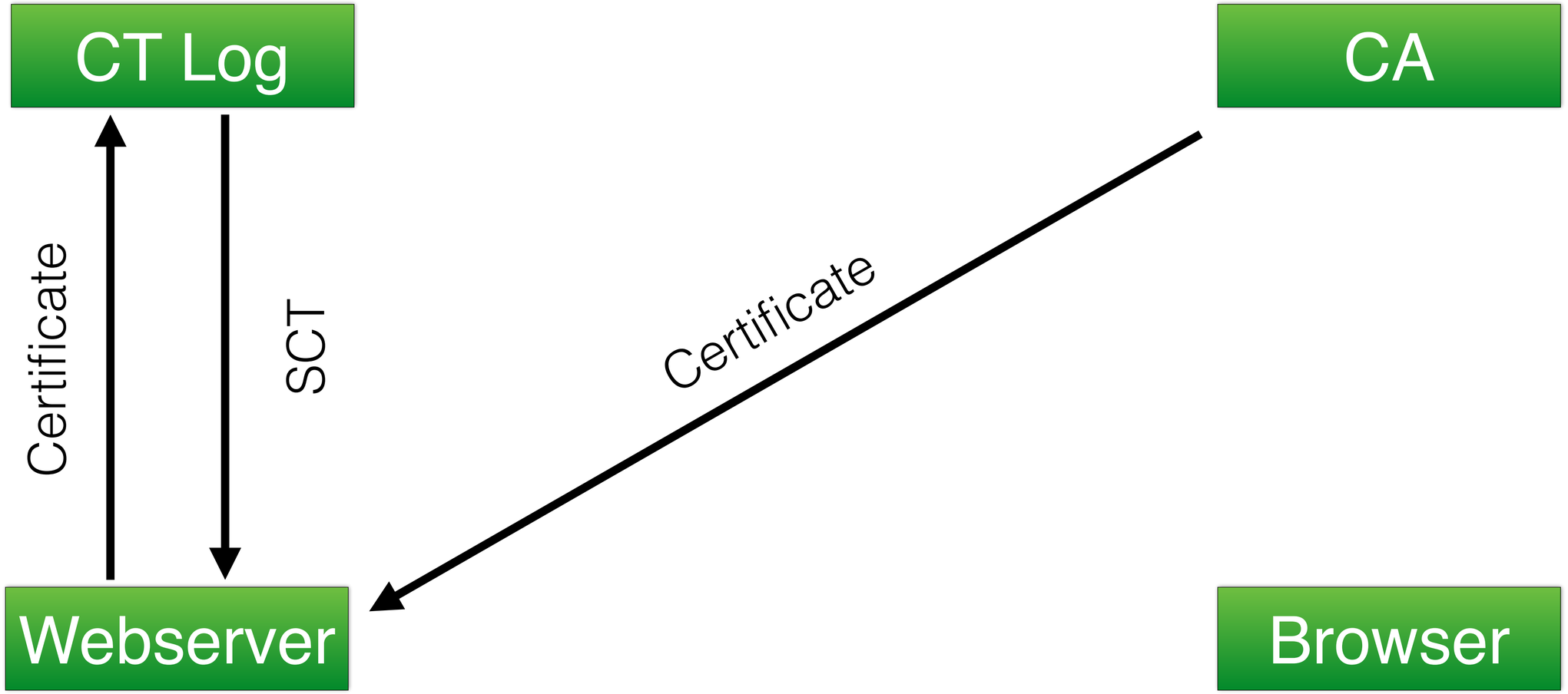
Certificate Transparency



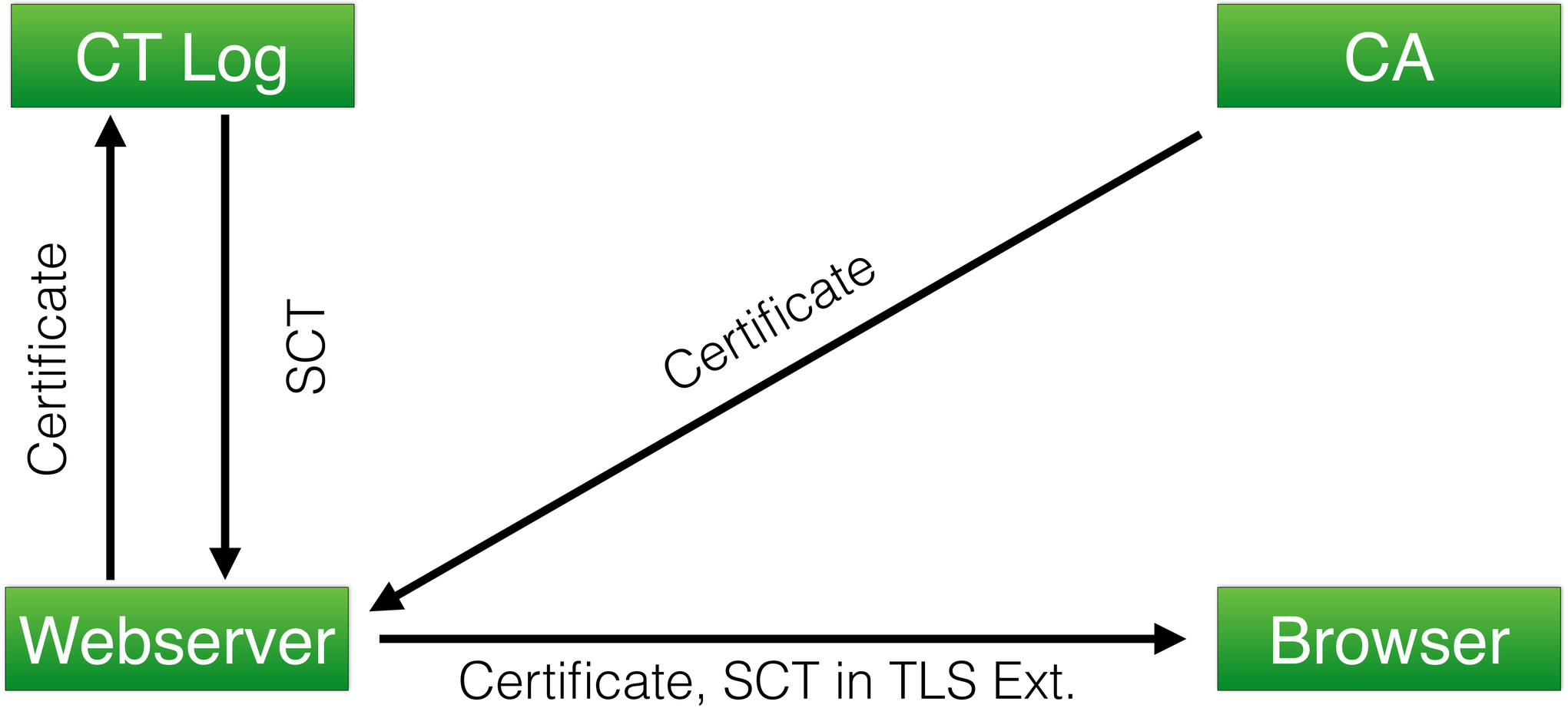
Certificate Transparency



Certificate Transparency



Certificate Transparency



Certificate Transparency

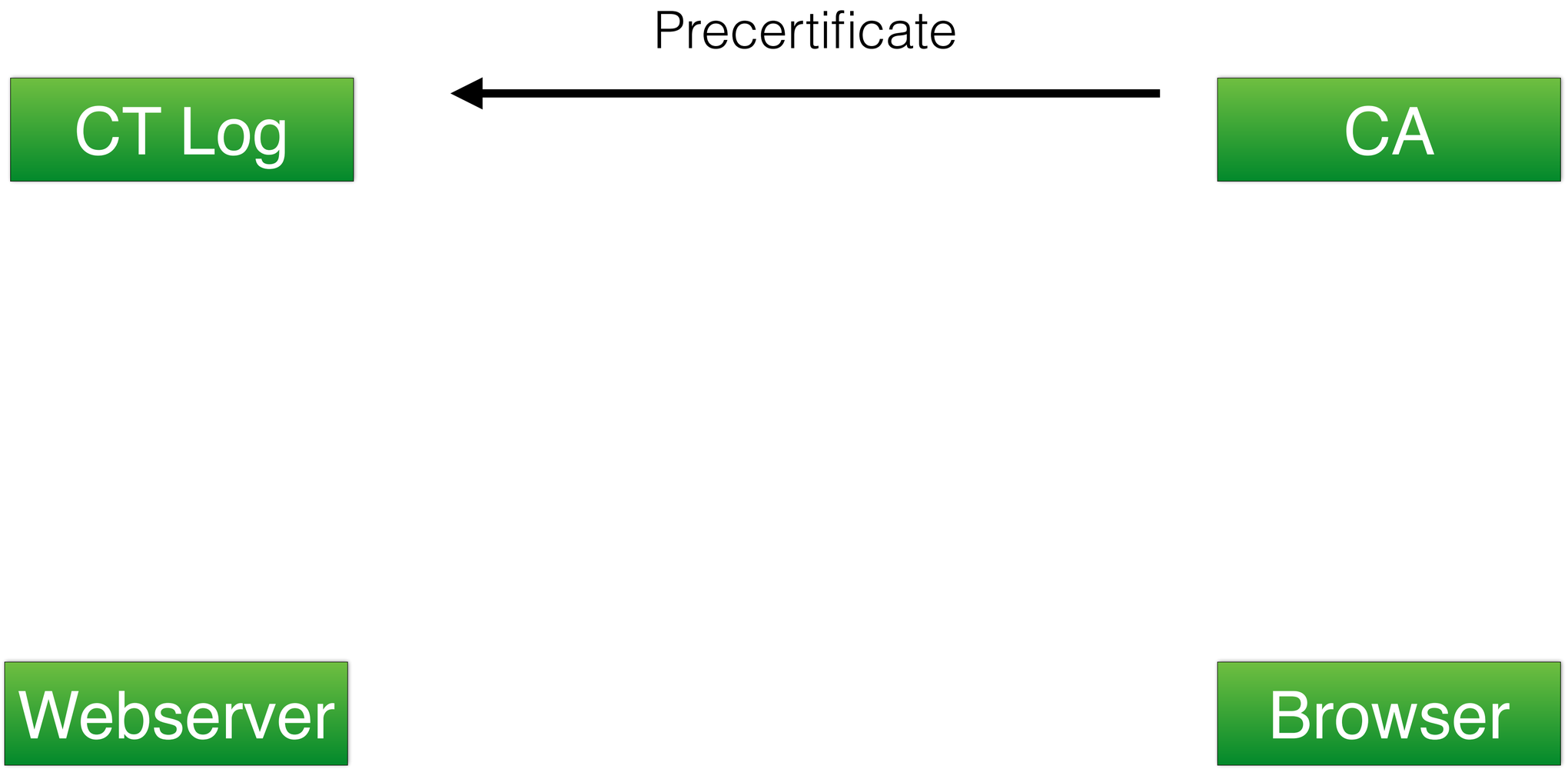
CT Log

CA

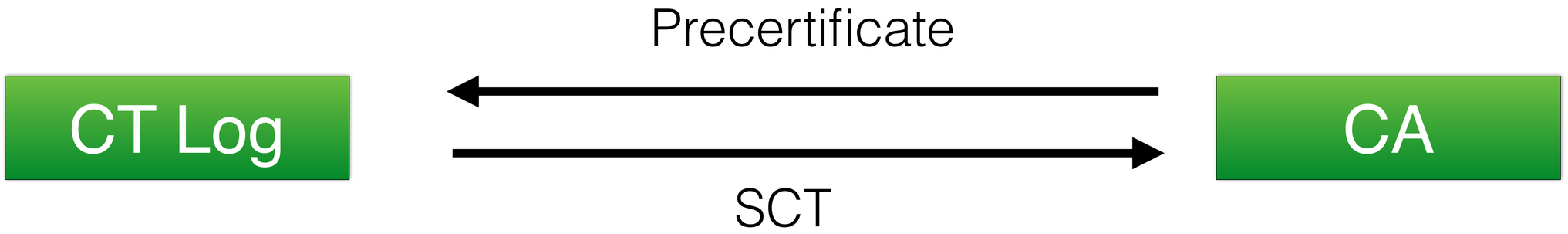
Webserver

Browser

Certificate Transparency



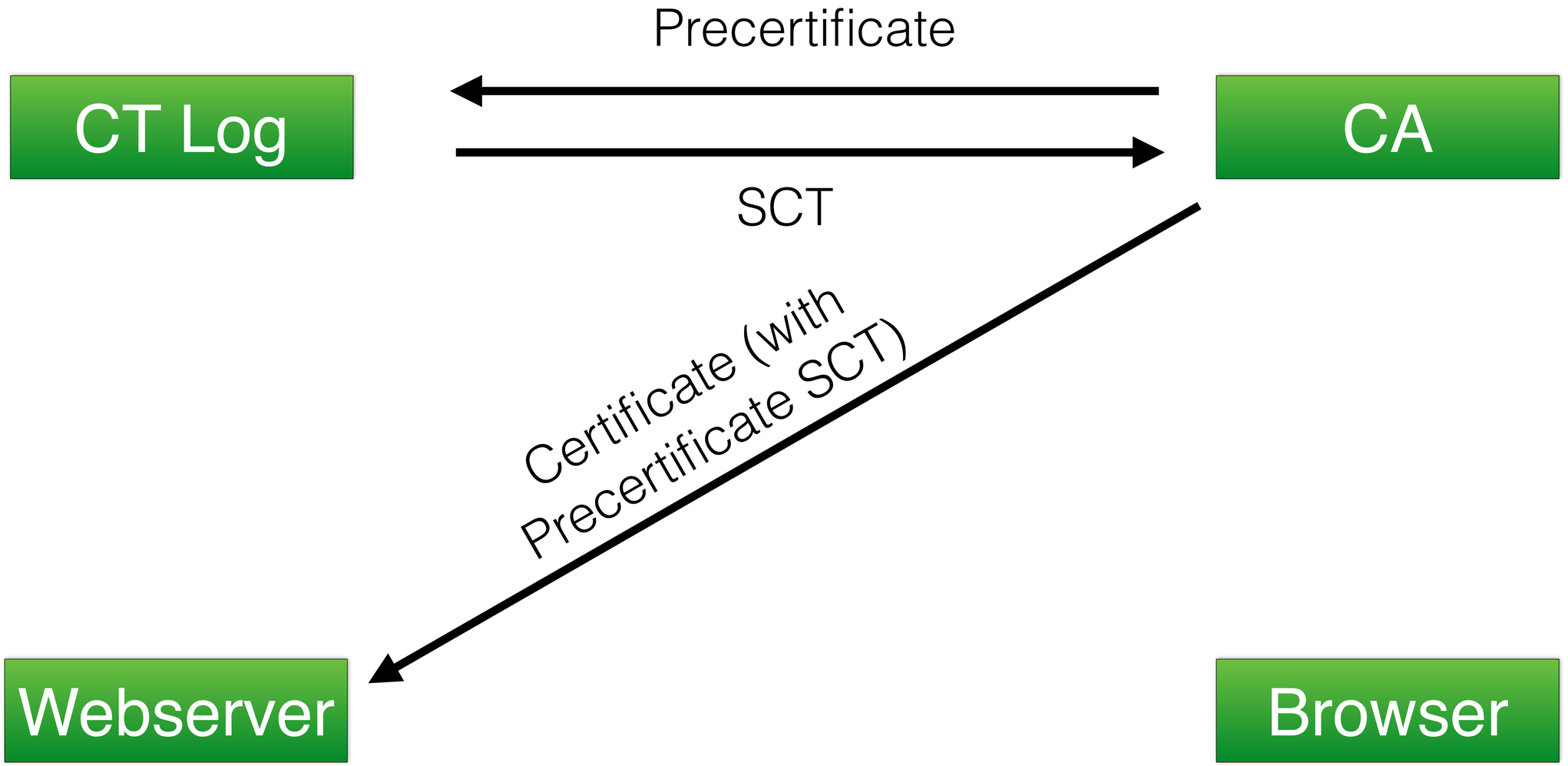
Certificate Transparency



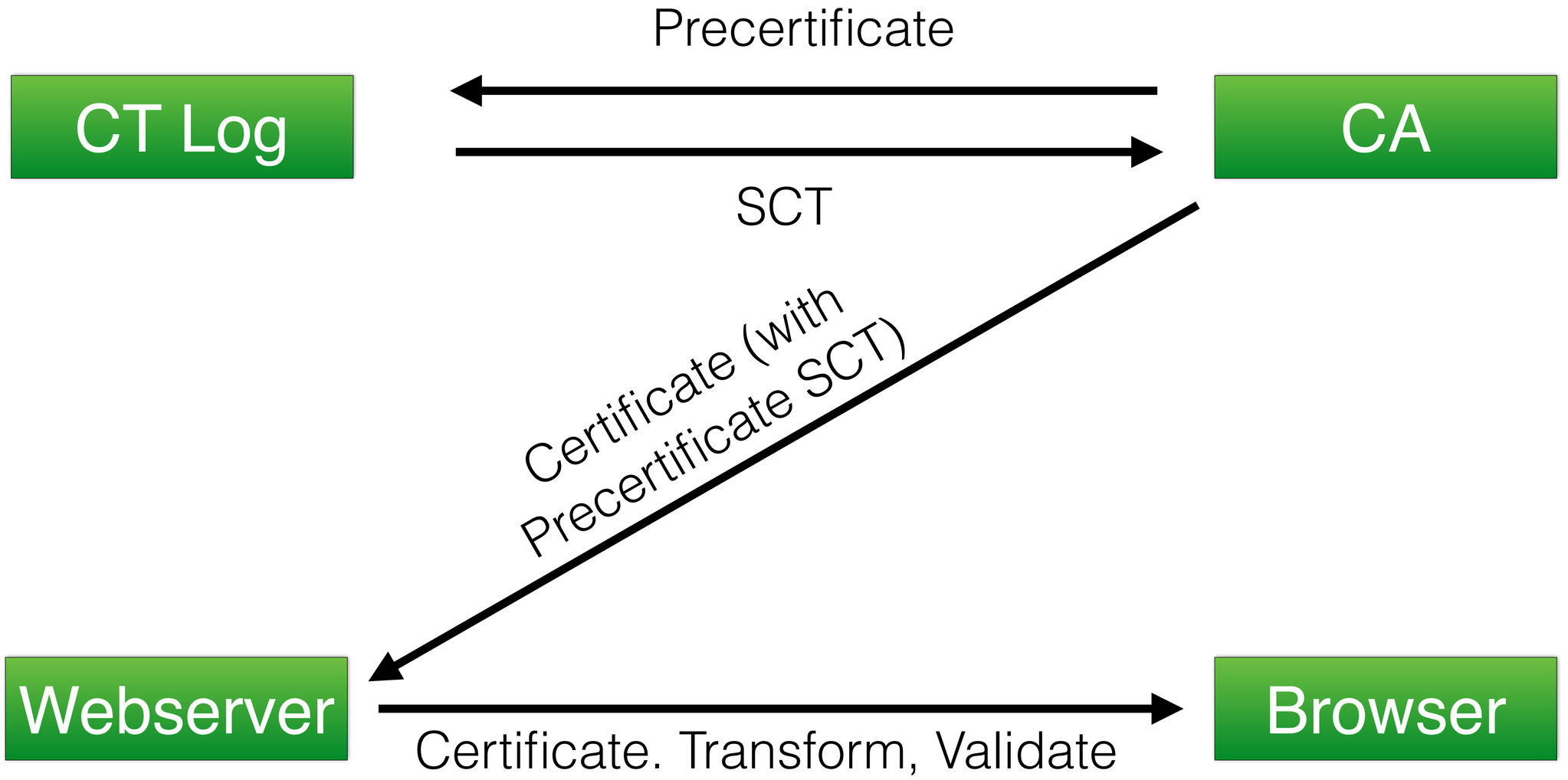
Webserver

Browser

Certificate Transparency



Certificate Transparency



Certificate Transparency

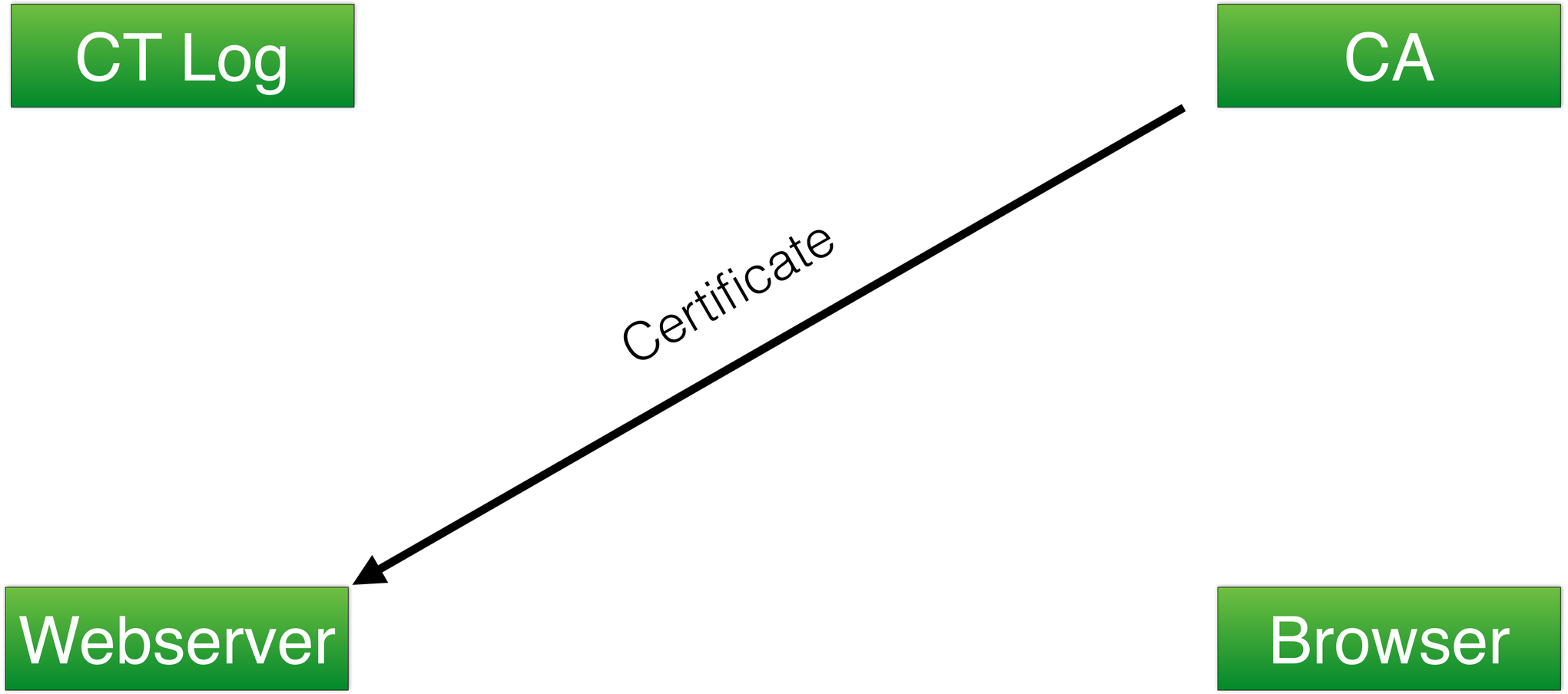
CT Log

CA

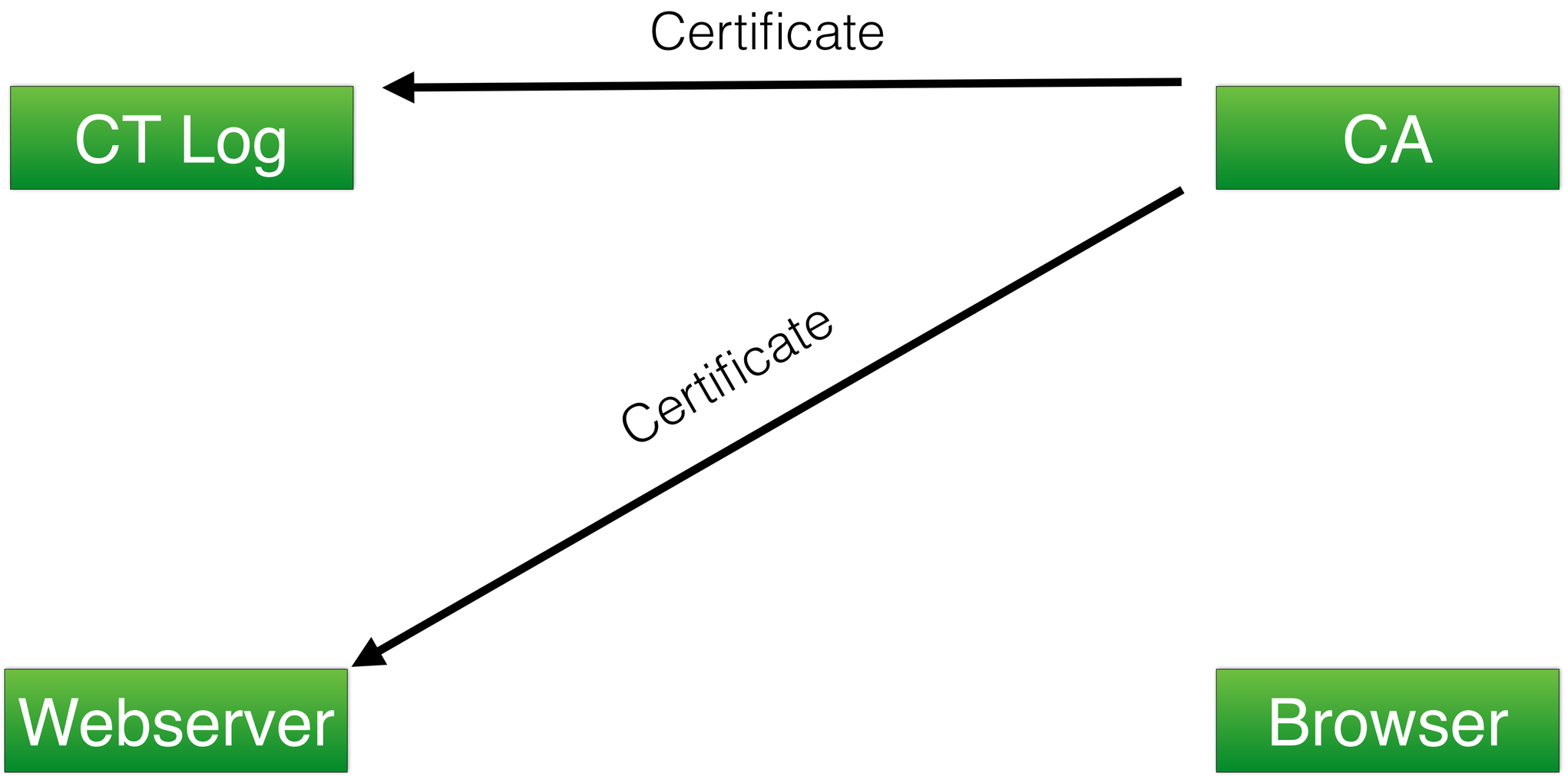
Webserver

Browser

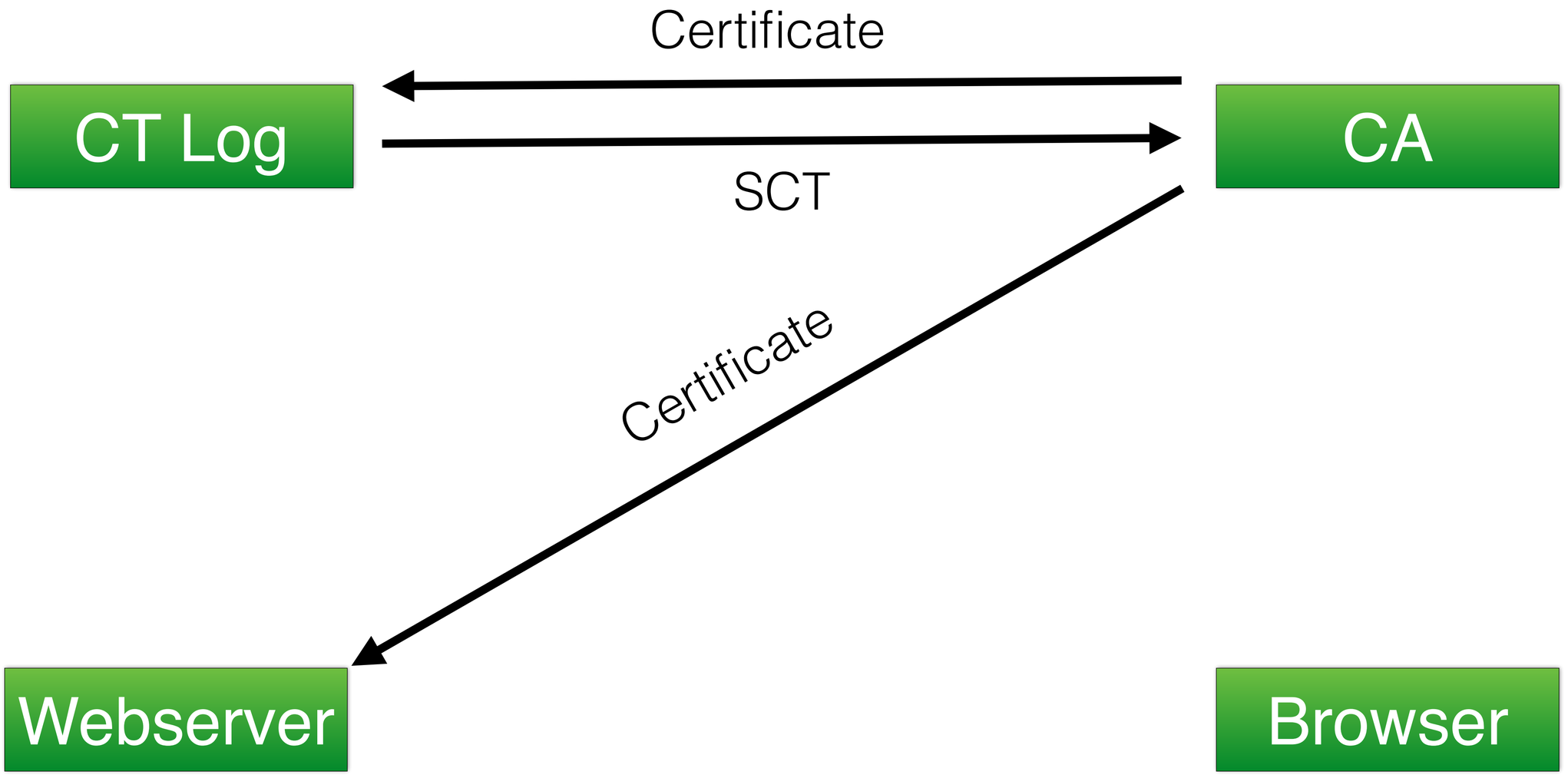
Certificate Transparency



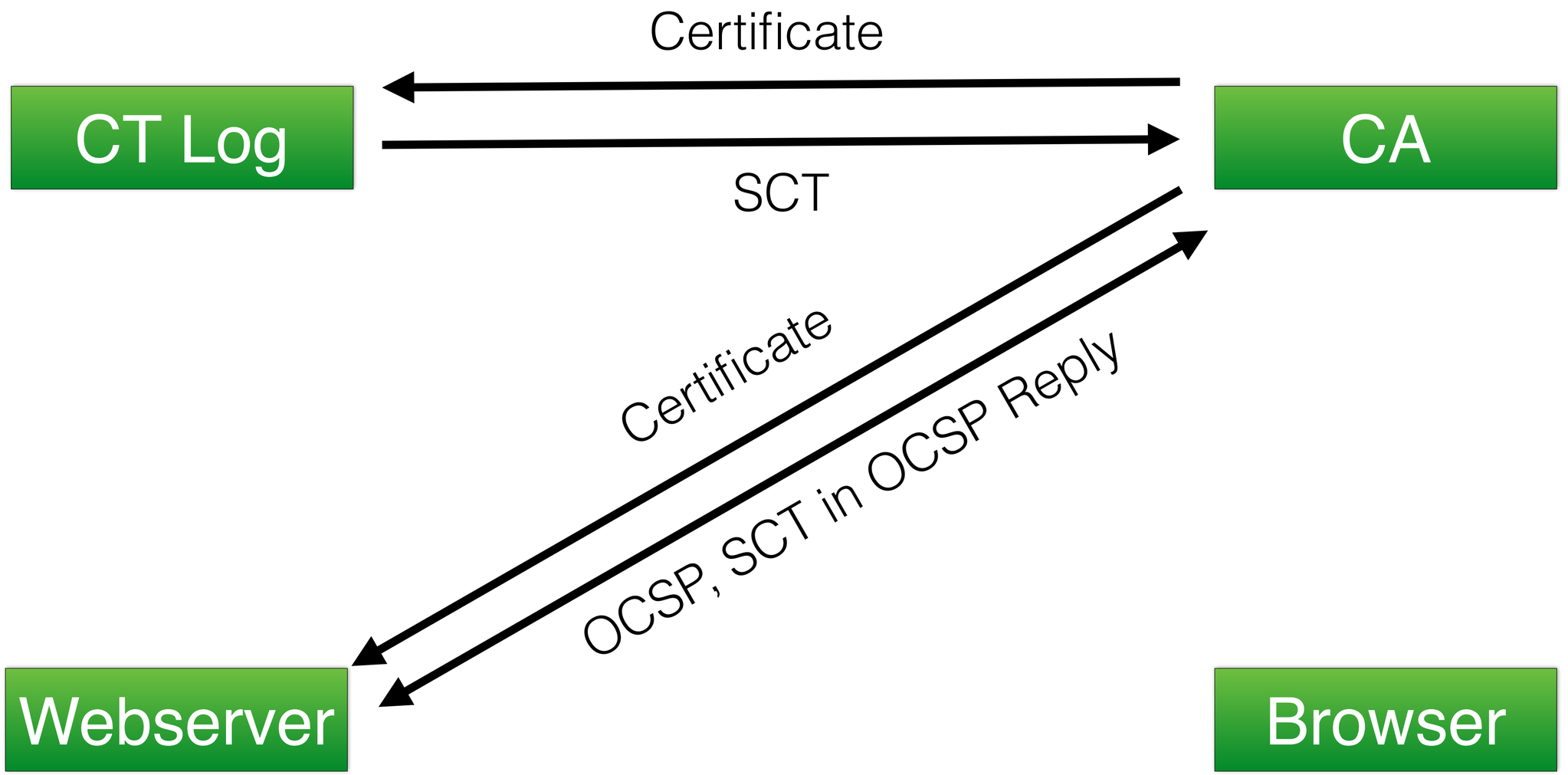
Certificate Transparency



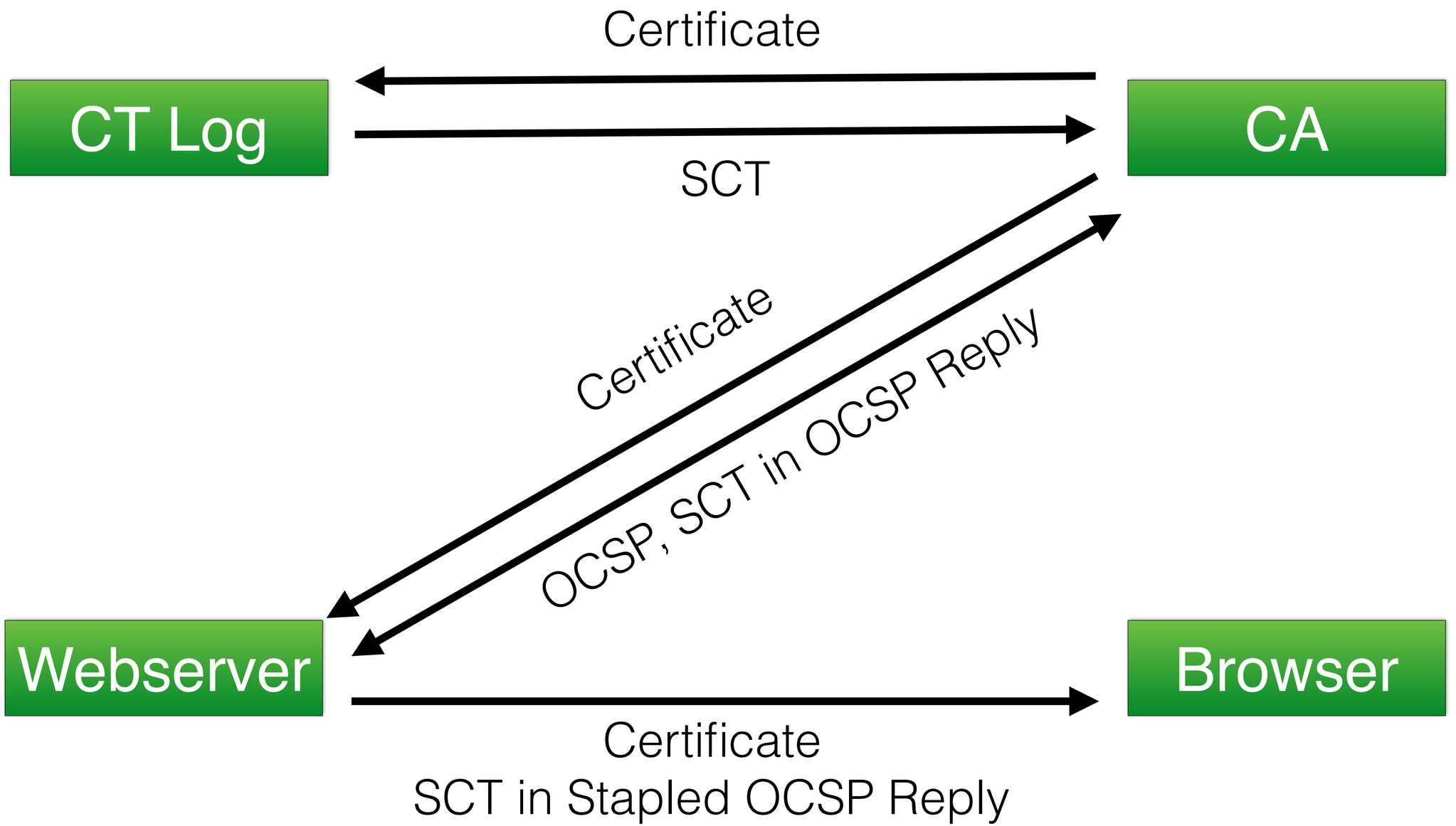
Certificate Transparency



Certificate Transparency



Certificate Transparency

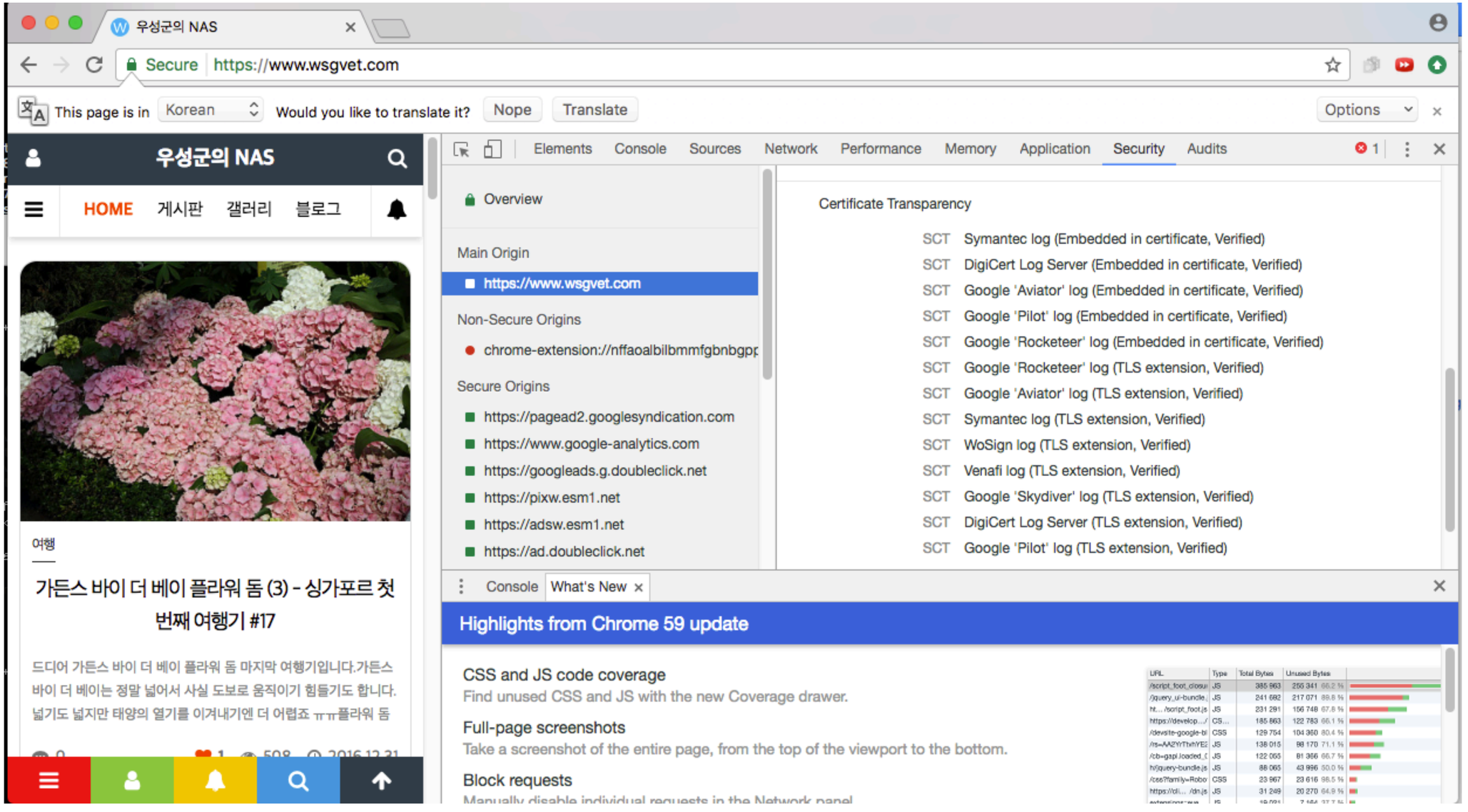


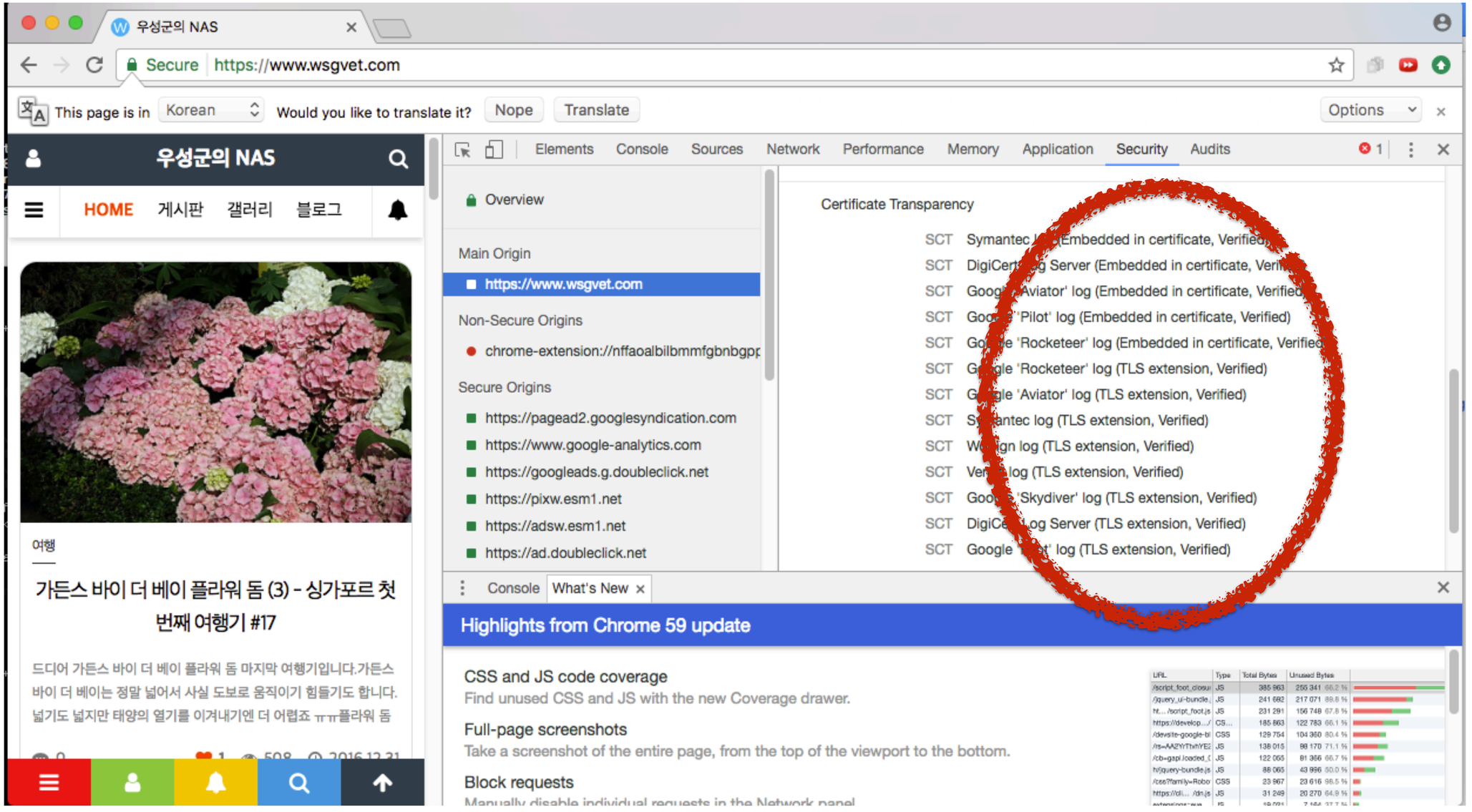
SCT Statistics - Active

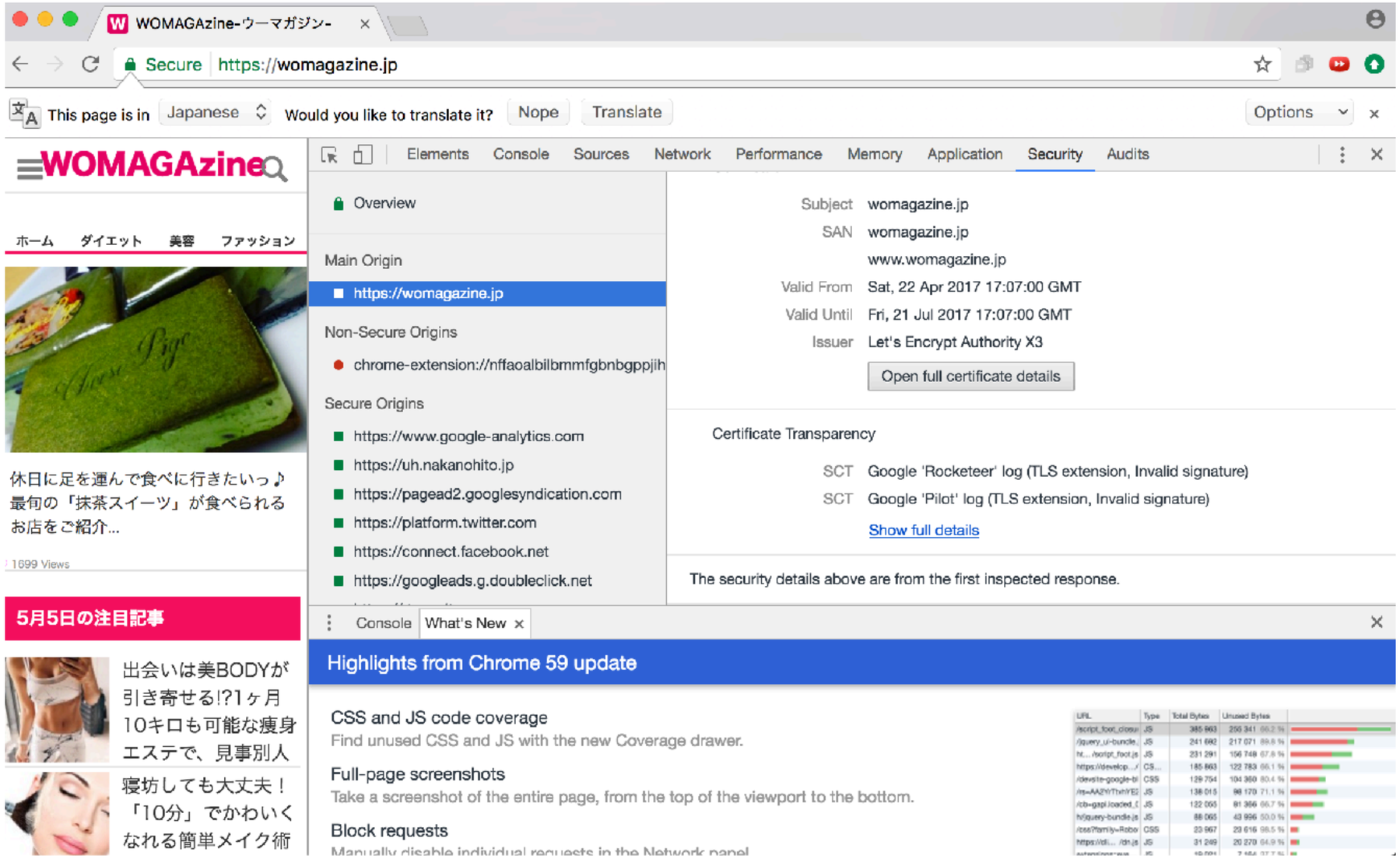
	Sydney v4	Munich v4	Munich v6
Domains we could connect to	55.7M	58.0M	5.1M
Domains with SCT	6.8M	6.8M	357K
… via X509	6.7M	6.8M	344K
… via TLS Ext.	27.6K	27.2K	12.9K
… via OCSP	180	188	3
Certificates (Total)	10.62M	9.66M	549.98K
Certificates with SCT Ext.	799.9K	834.5K	193.9K

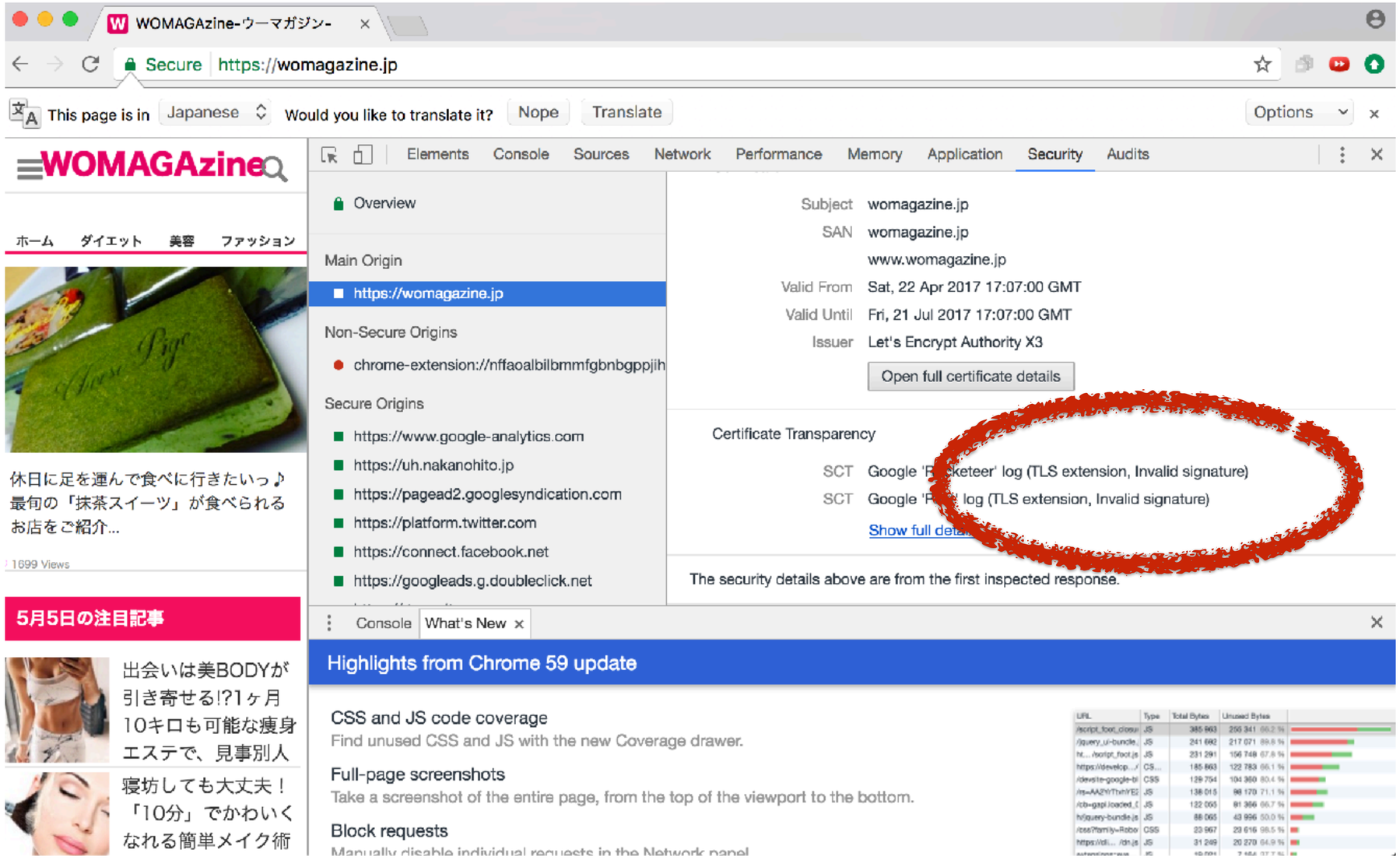
SCT Statistics - Passive

	California	Munich	Sydney
Time	4/4-5/2	5/12-5/16	5/12-5/16
Conns	2.6B	287M	196M
Conns with SCT	779M	73M	58M
… in Cert	520M	58M	44M
… in TLS	248M	14M	14M
… in OCSP	156K	38K	31K
# v4 IPs	737K	344K	226K
# SCT v4 IPs	222K	102K	66K

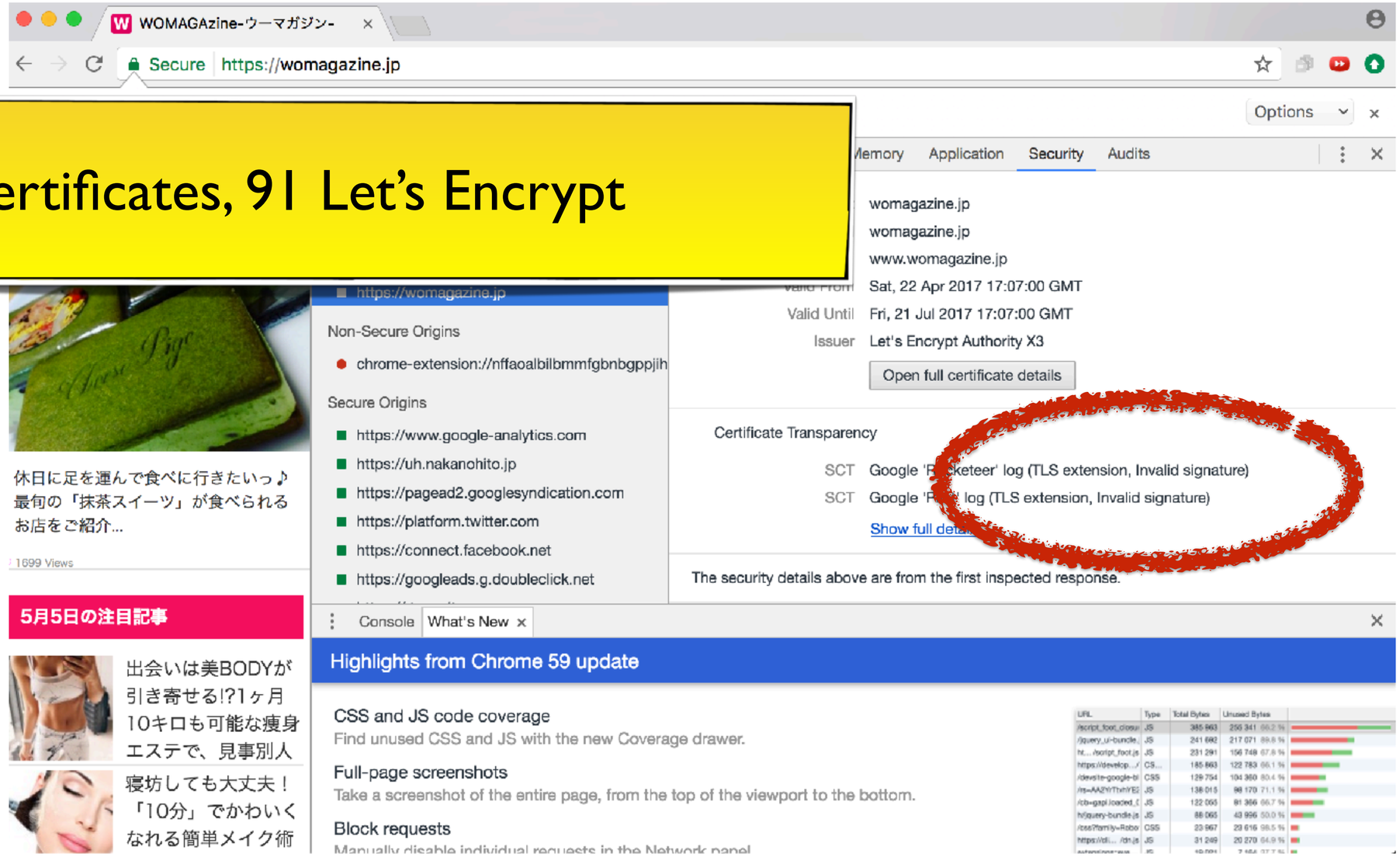

우성군의 NAS
Secure https://www.wsgvet.com
This page is in Korean Would you like to translate it? Nope Translate Options
우성군의 NAS
HOME 게시판 갤러리 블로그
여행
가든스 바이 더 베이 플라워 돔 (3) - 싱가포르 첫 번째 여행기 #17
드디어 가든스 바이 더 베이 플라워 돔 마지막 여행기입니다.가든스 바이 더 베이는 정말 넓어서 사실 도보로 움직이기 힘들기도 합니다. 넓기도 넓지만 태양의 열기를 이겨내기엔 더 어렵죠 ㅠㅠ플라워 돔
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://www.wsgvet.com
Non-Secure Origins
chrome-extension://nffaoalbilbmmfgbnbgpp
Secure Origins
https://pagead2.googlesyndication.com
https://www.google-analytics.com
https://googleads.g.doubleclick.net
https://pixw.esm1.net
https://adsw.esm1.net
https://ad.doubleclick.net
Certificate Transparency
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)
Console What's New
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

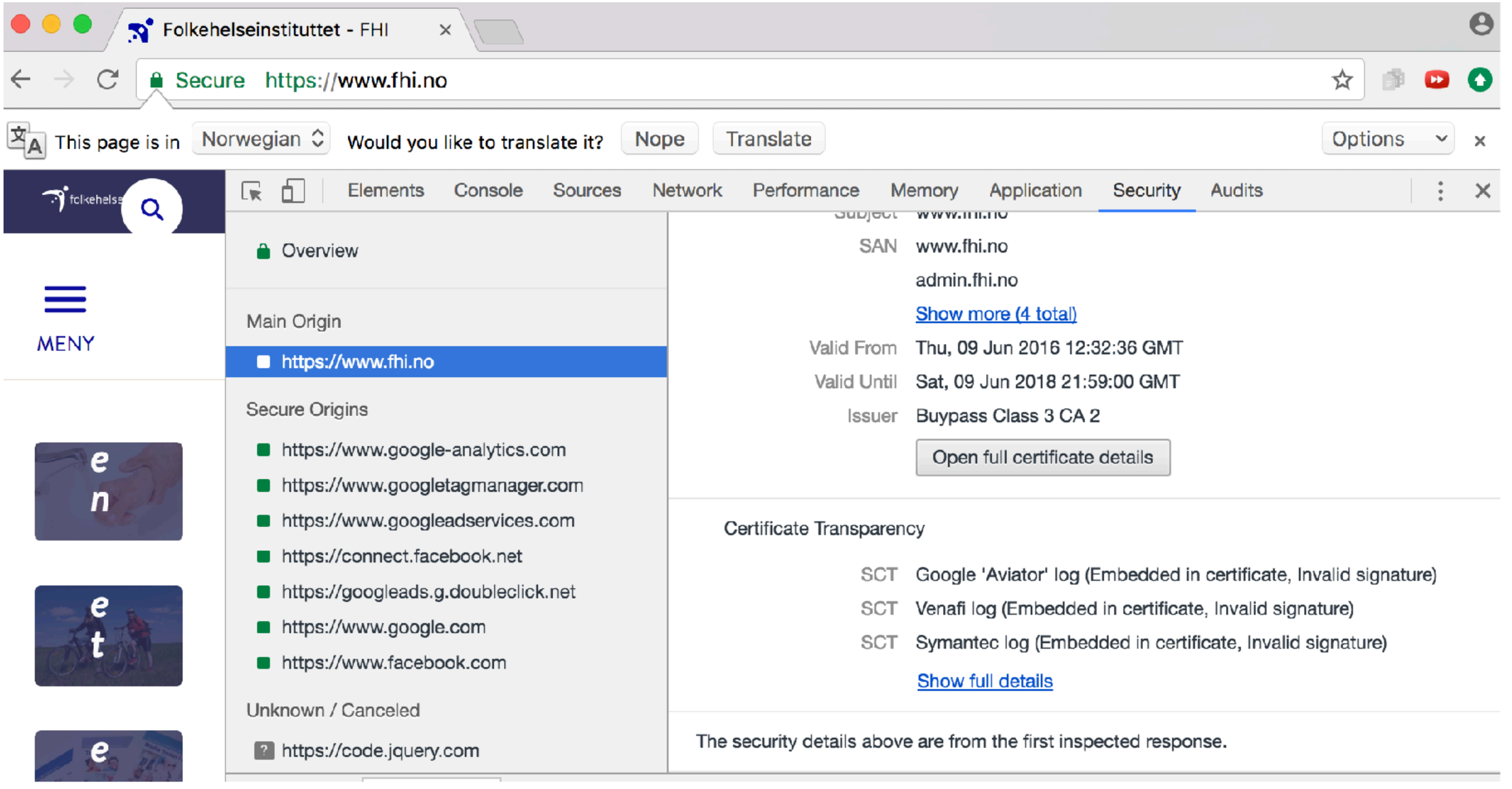

우성군의 NAS
Secure https://www.wsgvet.com
This page is in Korean Would you like to translate it? Nope Translate Options
우성군의 NAS
HOME 게시판 갤러리 블로그
여행
가든스 바이 더 베이 플라워 돔 (3) - 싱가포르 첫 번째 여행기 #17
드디어 가든스 바이 더 베이 플라워 돔 마지막 여행기입니다.가든스 바이 더 베이는 정말 넓어서 사실 도보로 움직이기 힘들기도 합니다. 넓기도 넓지만 태양의 열기를 이겨내기엔 더 어렵죠 ㅠㅠ플라워 돔
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://www.wsgvet.com
Non-Secure Origins
chrome-extension://nffaoalbilbmmfgbnbgpp
Secure Origins
https://pagead2.googlesyndication.com
https://www.google-analytics.com
https://googleads.g.doubleclick.net
https://pixw.esm1.net
https://adsw.esm1.net
https://ad.doubleclick.net
Certificate Transparency
SCT Symantec (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 Google log (TLS extension, Verified)
SCT Google 'Skydiver' log (TLS extension, Verified)
SCT DigiCert Log Server (TLS extension, Verified)
SCT Google log (TLS extension, Verified)
Console What's New
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

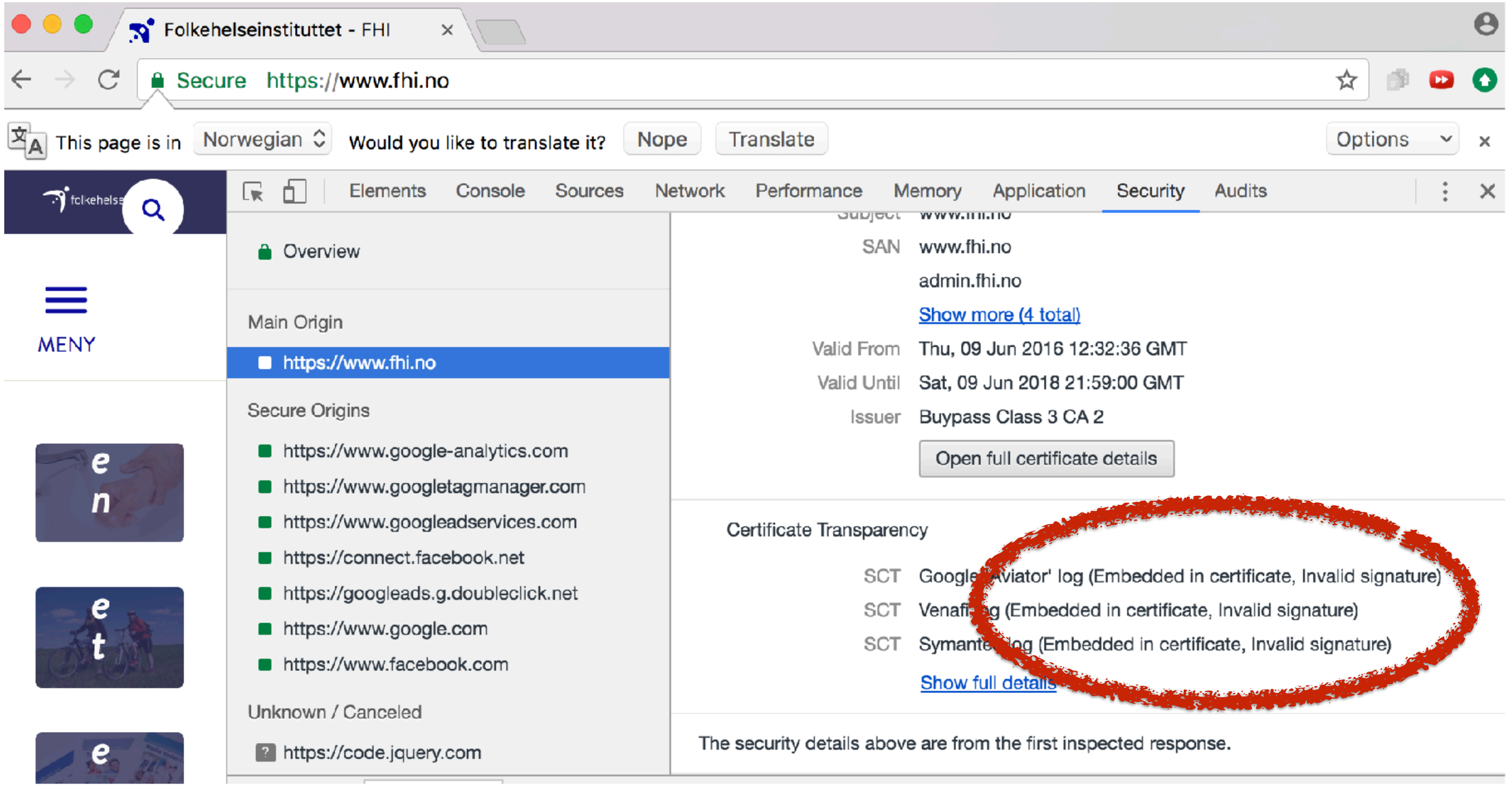

WOMAGAzine-ウーマガジン-
Secure https://womagazine.jp
This page is in Japanese Would you like to translate it? Nope Translate Options
WOMAGAzine
ホーム ダイエット 美容 ファッション
休日に足を運んで食べに行きたいっ♪ 最旬の「抹茶スイーツ」が食べられるお店をご紹介...
1699 Views
5月5日の注目記事
出会いは美BODYが引き寄せる!?1ヶ月10キロも可能な痩身エステで、見事別人
寝坊しても大丈夫！「10分」でかわいくなれる簡単メイク術
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://womagazine.jp
Non-Secure Origins
chrome-extension://nffaoalbilbmmfgbnbgppjih
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
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


WOMAGAzine-ウーマガジン-
Secure https://womagazine.jp
This page is in Japanese Would you like to translate it? Nope Translate Options
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...
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
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://womagazine.jp
Non-Secure Origins
chrome-extension://nffaoalbilbmmfgbnbgppjih
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 'R keteer' log (TLS extension, Invalid signature)
SCT Google 'P log (TLS extension, Invalid signature)
Show full deta
The security details above are from the first inspected response.
Console What's New
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

105 Certificates, 91 Let's Encrypt



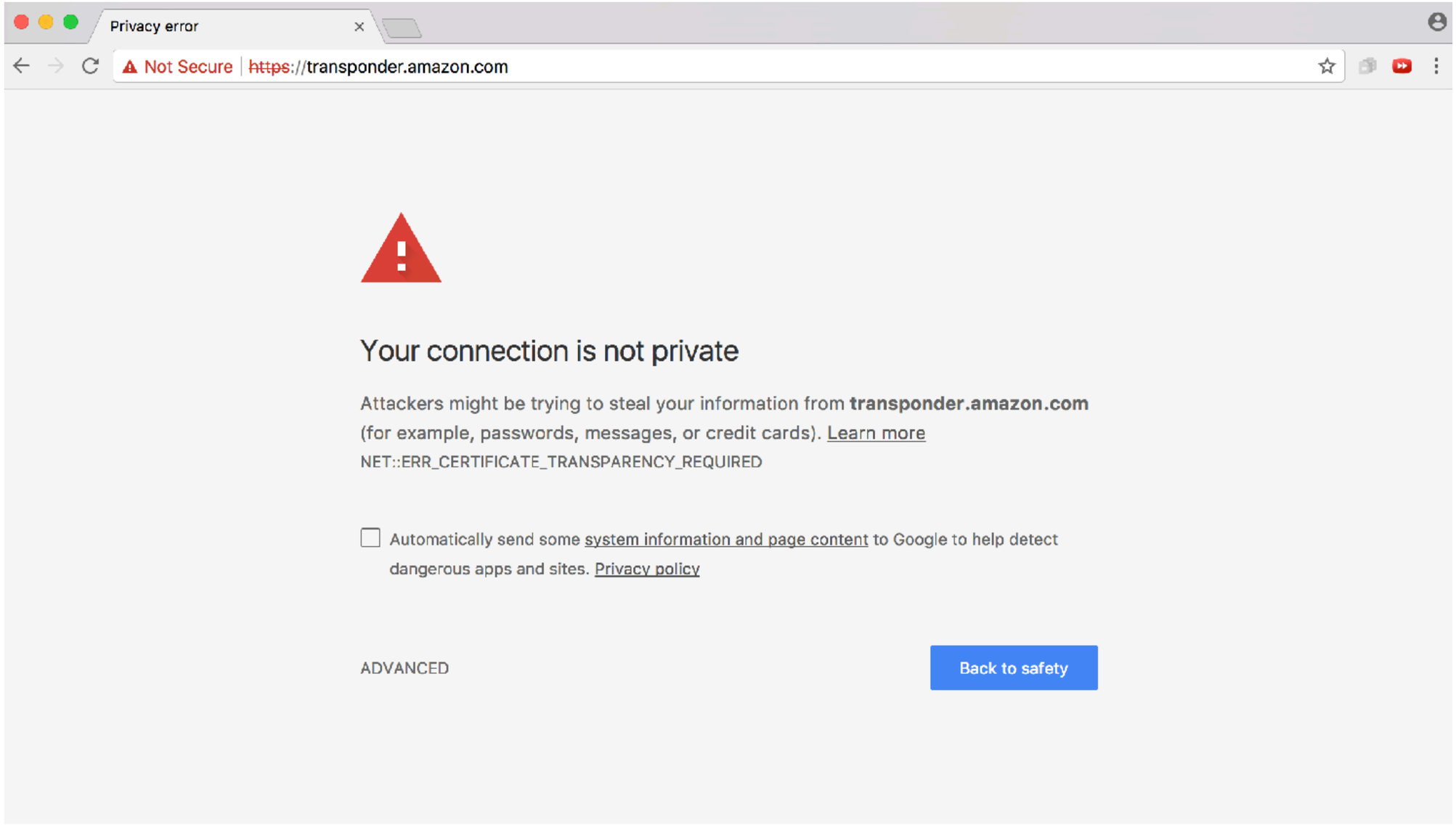

Folkehelseinstituttet - FHI
Secure https://www.fhi.no
This page is in Norwegian Would you like to translate it? Nope Translate Options
MENY
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://www.fhi.no
Secure Origins
https://www.google-analytics.com
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
SAN www.fhi.no
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.


Folkehelseinstituttet - FHI
Secure https://www.fhi.no
This page is in Norwegian Would you like to translate it? Nope Translate Options
MENY
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
SAN www.fhi.no
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 (Embedded in certificate, Invalid signature)
SCT (Embedded in certificate, Invalid signature)
SCT (Embedded in certificate, Invalid signature)
Show full details
The security details above are from the first inspected response.

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

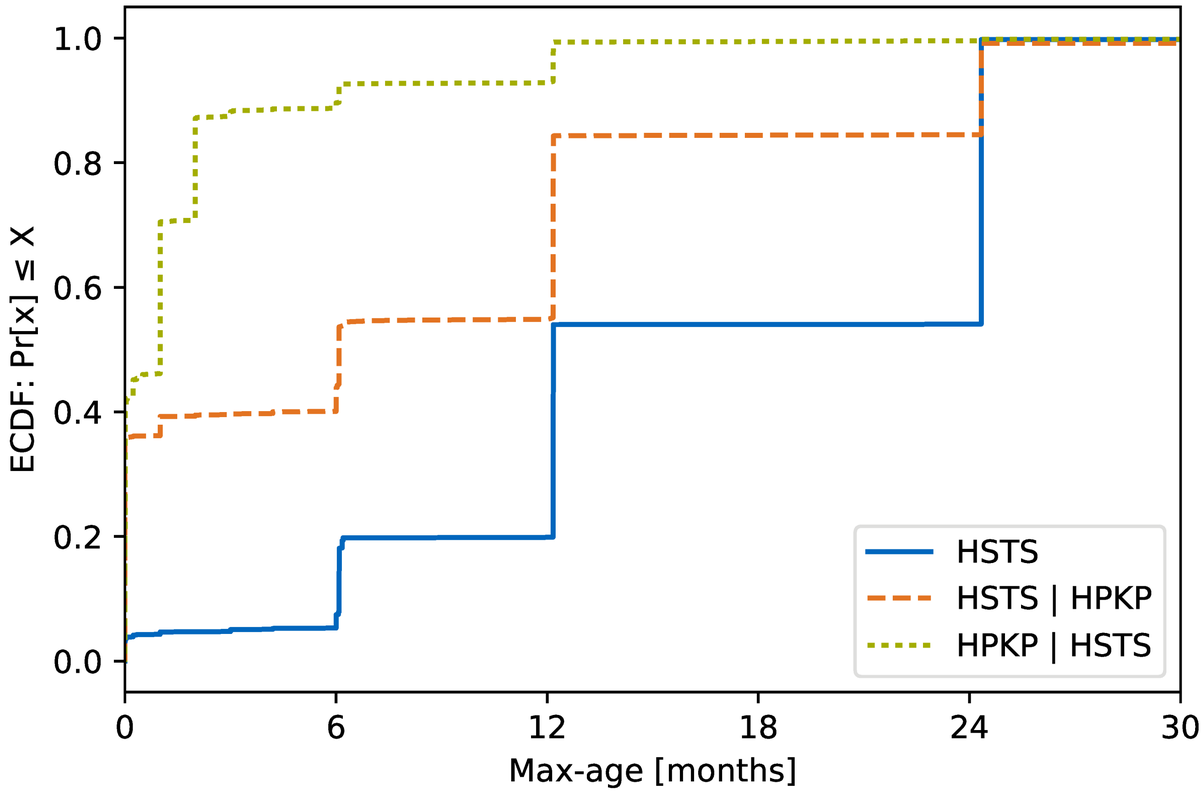


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            36:9a:c7:3d:67:06:3a:a2:75:83:0d:fc:66:84:1c:1e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
 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

```
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
```

HSTS, HPKP

- HSTS: ~3.5% of domains
  - 0.2% send incorrect headers (misspellings, wrong attributes, …)
- HPKP: ~0.02% of domains (6,181)
  - 41 invalid



SCSV

Automatically deployed when servers/libraries update

> 96% deployment

Deployment

Mechanism	Standard-ized	Deployment Overall	Deployment Top 10K↓	Effort	Availability Risk
SCSV	2015	49.2M	6789	**none**	low
CT-x509	2013	7.0M	1788	**none**[2]	**none**
HSTS	2012	0.9M	349	low	low
CT-TLS	2013	27,759	171	high	**none**
HPKP	2015	6616	156	high	high
HPKP PL.	2012[1]	479	150	high	high
HSTS PL.	2012[1]	23,539	144	medium	medium
CAA	2013	3057	20	medium	low
TLSA	2012	973	3	high	medium
CT-OCSP	2013	191	0	low	**none**

1: Preloading list first added to Chrome in 2012

2: Requires deployment effort on CA side and a new site certificate.

Intent To Deprecate And Remove: Public Key Pinning

31 posts by 14 authors

Chris Palmer Oct 27

Primary eng (and PM) emails

palmer@chromium.org, rsleevi@chromium.org, estark@chromium.org, agl@chromium.org

Summary

Deprecate support for public key pinning (PKP) in Chrome, and then remove it entirely.

This will first remove support for HTTP-based PKP ("dynamic pins"), in which the user-agent learns of pin-sets for hosts by HTTP headers. We would like to do this in Chrome 67, which is estimated to be released to Stable on 29 May 2018.

Finally, remove support for built-in PKP ("static pins") at a point in the future when Chrome requires Certificate Transparency for all publicly-trusted certificates (not just newly-issued publicly-trusted certificates). (We don't yet know when this will be.)

Community Contributions

- PCAPs of active scans
- Active scan results, CT database dumps
- Analysis Scripts (primarily Jupyter notebooks)
- Datasets: https://mediatum.ub.tum.de/1377982
- Software:
  - goscanner (HTTPS scanner): https://github.com/tumi8/goscanner
  - extended Bro TLS support (in master): https://bro.org

Summary

- Deployment status correlates with:
  - Configuration effort
  - Risk
  - Default deployment / settings work best
- Measurements from several sites have very similar results
  - One measurement location probably good enough in most cases