# Certificate Transparency: Warum macht Google das?

Diana Topko

HAW Seminar

26.04.2016

# Übersicht

- Was ist CT?
- CT-Komponenten
- Certificate Logs
- Vorteile und Mängel
- Zusammenfassung

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# Was ist Certificate Transparency?

- Certificate Transparency ist ein offenes, von Google vorangetriebenes Framework für das Überprüfen von digitalen Zertifikaten
- Die Zertifizierungsstellen sollen durch Certificate Transparency daran gehindert werden digitale Zertifikate für eine Domain auszustellen ohne vorher den Eigentümer der Domain hierüber zu informieren

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# Was ist Certificate Transparency?

Erste vollständige Beschreibung vom CT-Framework wurde im Juni 2013 von B. Laurie, A. Langley und E. Kasper bei der IETF als “Experimental Request for Comments:6962” eingereicht

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# Was ist Certificate Transparency?

Extended-Validation-Zertifikate, die nach dem 1. Januar 2015 ohne Certificate Log vom Zertifikatsanbieter ausgestellt werden, zeigt der Google Chrome Browser nicht mehr als sicher an.

# Was ist Certificate Transparency?

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

Transparenz wird dadurch erreicht, dass Zertifizierungsstellen die Zertifikate auf öffentlich zugängliche qualifizierte Certifikate Logs registrieren.

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# Wie funktioniert Certificate Transparency?

Wenn ein gültiges Zertifikat einem Certificate Log vorgelegt wird, antwortet das Log mit einem signierten Zeitstempel - SCT
SCT stellt die Zusicherung dar, das Zertifikat innerhalb eines bestimmten Zeitabschnitts - maximale „Einbringungsverzögerung”, zum Certificate Log hinzugefügt wird

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# Gründe für Certificate Transparency

## Warum sind SSL/TLS Zertifikate wichtig?

- SSL/TLS Zertifikate bieten vertraulichen Ende-zu-Ende-Verschlüsselung bei der Datenübertragung
- SSL/TLS Zertifikate prüfen die Vertrauenswürdigkeit des Webseitenbetreibers und vermitteln diese dem Besucher der Webseite

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# Gründe für Certificate Transparency

- Der Browser **kann** die Webseiten mit ungültige Zertifikaten erkennen
- Der Browser **kann nicht** erkennen, wenn die Webseiten über irrtümlich ausgestellte Zertifikate verfügen oder wenn diese über Zertifikate verfügen, welche von einer manipulierten Zertifizierungsstelle ausgestellt wurden.

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# Hauptziele des CT-Projekts:

1. Es soll für eine Zertifizierungsstelle unmöglich (oder zumindest sehr schwer) sein, ein SSL-Zertifikat für eine Domain auszustellen, ohne dass das Zertifikat für den Eigentümer dieser Domain sichtbar ist.

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# Hauptziele des CT-Projekts:

2. Ein offenes Überprüfungs- und Überwachungssystem bereitzustellen, mit dem alle Domain-Inhaber oder Zertifizierungsstellen feststellen können, ob falsche Zertifikate irrtümlich oder vorsätzlich ausgestellt wurden.

**Was ist CT?**

CT-Komponenten

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# Hauptziele des CT-Projekts:

3. Benutzer davor zu schützen durch Zertifikate, die irrtümlich oder vorsätzlich ausgestellt wurden, betrogen zu werden.

- Benutzerdaten vom Zugriff eines Dritten durch Ende-zu-Ende-Verschlüsselung zu schützen
- Die Vertrauenswürdigkeit des Webseite-Betreibers durch die Authentifizierung zu gewährleisten

Was ist CT?

**CT-Komponenten**

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# CT-Framework besteht aus drei Komponenten:

- Certificate Logs
- Monitore
- Auditore

Was ist CT?

**CT-Komponenten**

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# CT-Komponenten

## Certificate Logs

- „Append-only“ Eigenschaft (mit Zeitstempel)
- Kryptografisch gesichert
- Öffentlich auditierbar

# CT-Komponenten



Certificate Logs verwenden Merkle-Hash Trees

Was ist CT?

**CT-Komponenten**

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# CT-Komponenten

## Monitore

- Setzen sich in regelmäßigen Zeitabständen mit allen Certificate Logs in Verbindung
- Suchen nach verdächtigen Zertifikaten

Was ist CT?

**CT-Komponenten**

Certificate Logs

Vorteile und Mängel

Zusammenfassung

# CT-Komponenten

## Auditore

- Softwarekomponenten
- Prüfen, ob sich Certificate Logs korrekt verhalten und kryptografisch konsistent sind
- Prüfen, ob ein bestimmtes Zertifikat in einem von bekannten Certificate Logs erscheint

# CT-Komponenten



- X.509v3 Extension
- TLS Extension
- OCSP Stapling

Was ist CT?

**CT-Komponenten**

Certificate Logs

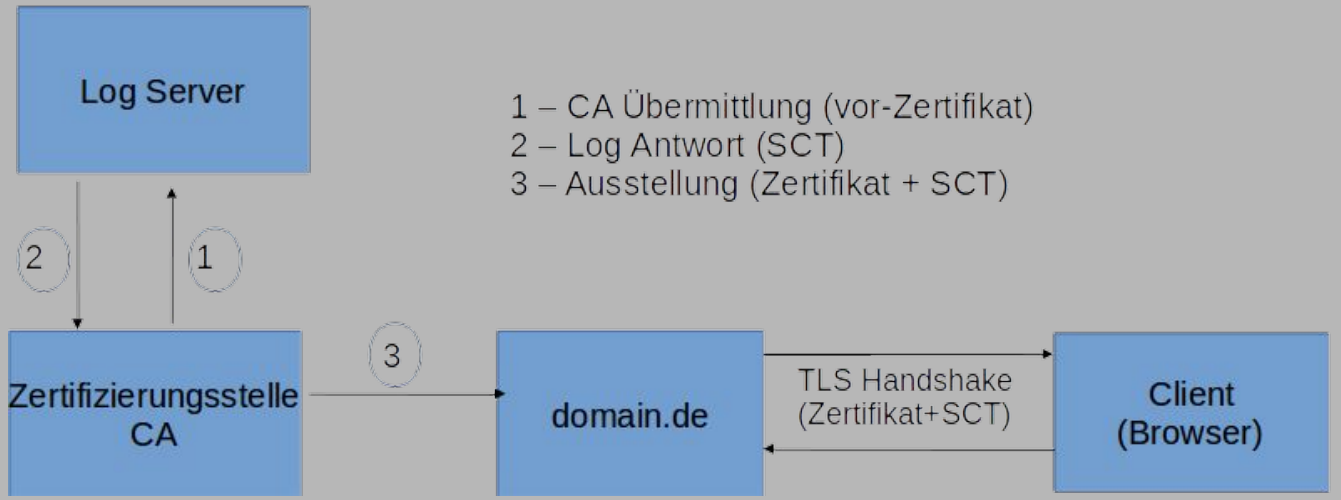
Vorteile und Mängel

Zusammenfassung

## Funktionsweise von TLS/SSL ohne Certificate Transparency


X.509v3 Extension

## Funktionsweise von TLS/SSL mit Certificate Transparency



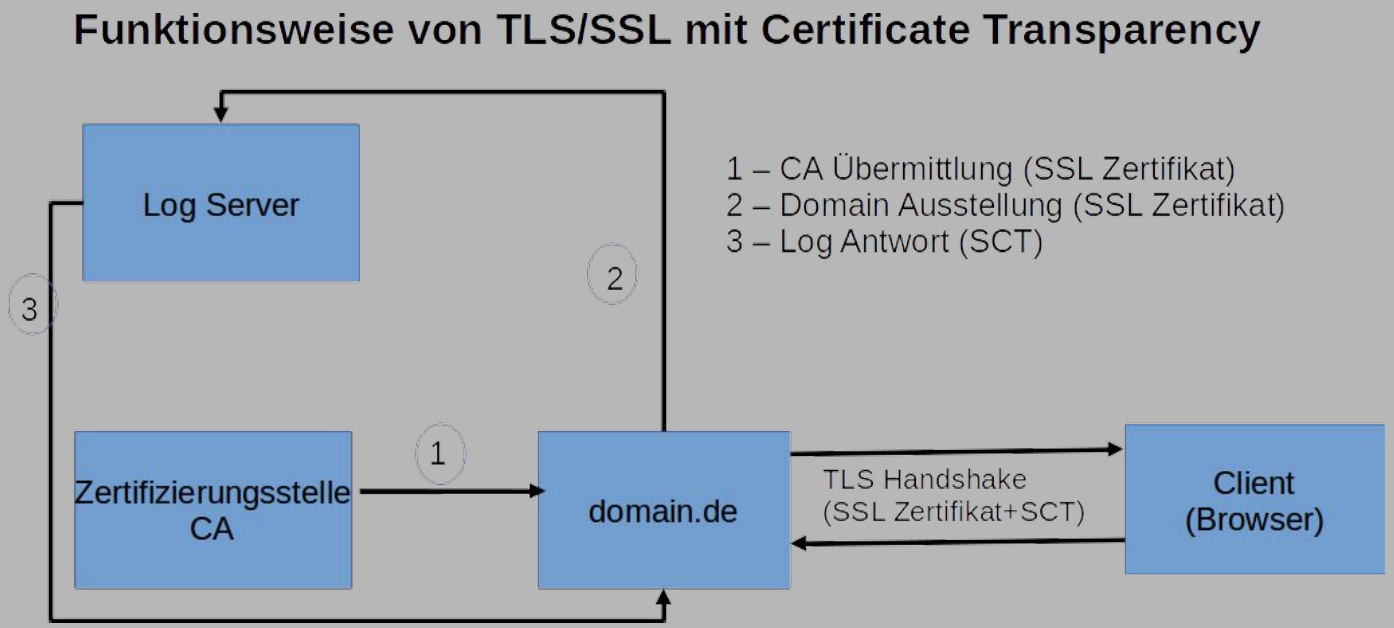
Was ist CT?

**CT-Komponenten**

Certificate Logs

Vorteile und Mängel

Zusammenfassung



Was ist CT?

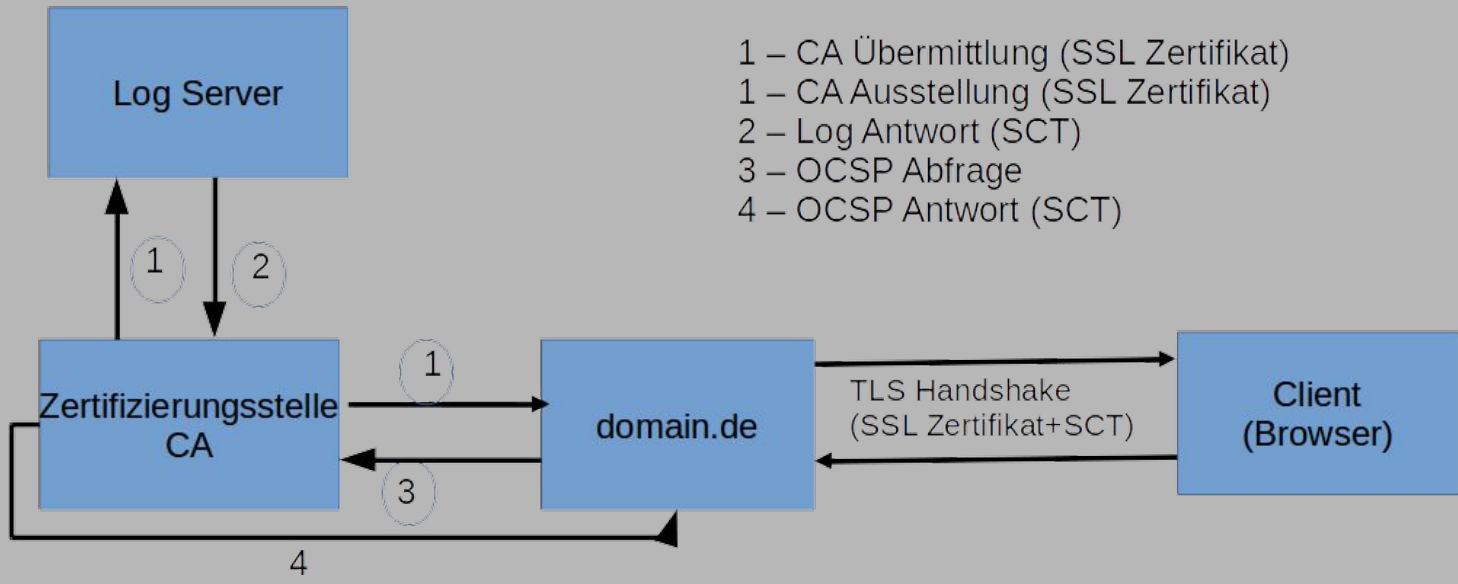
**CT-Komponenten**

Certificate Logs

Vorteile und Mängel

Zusammenfassung

## Funktionsweise von TLS/SSL mit Certificate Transparency



Was ist CT?

CT-Komponenten

**Certificate Logs**

Vorteile und Mängel

Zusammenfassung

# Interaktion mit Certificate Logs

Jeder kann via HTTPS GET-und POST-Meldungen Zertifikate vom Certificate Log abfragen und zum Certificate Log hinzufügen

Was ist CT?

CT-Komponenten

**Certificate Logs**

Vorteile und Mängel

Zusammenfassung

# Interaktion mit Certificate Logs

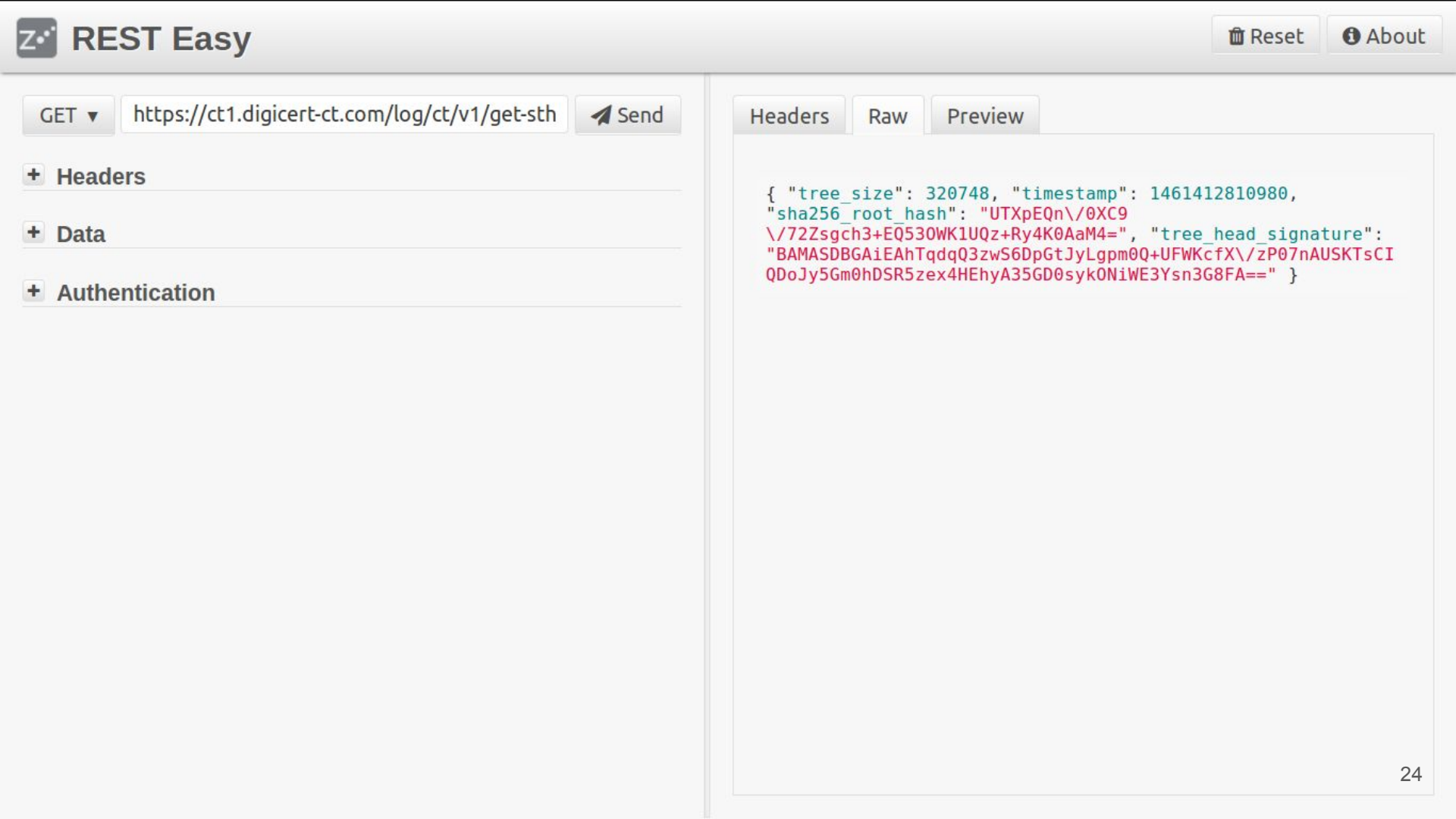
**GET** https://ct1.digicert-ct.com/log/ct/v1/get-sth

Liefert

- Baumgröße mit Anzahl von Einträgen in Log
- Den Zeitstempel vom letzten Eintrag
- Merkle Tree Hash Wert von dem Baum
- Tree Head Signature

**Dokumentation:**

Request for Comments: 6962


REST Easy
Reset
About
GET
https://ct1.digicert-ct.com/log/ct/v1/get-sth
Send
Headers
Data
Authentication
Headers
Raw
Preview
{ "tree_size": 320748, "timestamp": 1461412810980,
"sha256_root_hash": "UTXpEQn\/0XC9
\/72Zsgch3+EQ53OWK1UQz+Ry4K0AaM4=", "tree_head_signature":
"BAMASDBGAiEAhTqdqQ3zwS6DpGtJyLgpm0Q+UFWKcfX\/zP07nAUSKTsCI
QDoJy5Gm0hDSR5zex4HEhyA35GD0sykONiWE3Ysn3G8FA==" }
24

Was ist CT?

CT-Komponenten

**Certificate Logs**

Vorteile und Mängel

Zusammenfassung

# Interaktion mit Certificate Logs

-Beispiele von Certificate Logs

- ct.googleapis.com/aviator
- ct.googleapis.com/pilot
- ct1.digicert-ct.com/log
- vega.ws.symantec.com

-Vollständige Auflistung von Certificate Logs:
https://www.certificate-transparency.org/known-logs

Was ist CT?

CT-Komponenten

**Certificate Logs**

Vorteile und Mängel

Zusammenfassung

# NetLog von Chrome

Detaillierte Information zum Signed Certificate Timestamp wird in NetLog von Google Chrome angezeigt.

chrome://net-internals

Events ▾ capturing events (14985)

(?) 655 of 655

| | | | |
|---|---|---|---|
| | 5185 | URL_REQUEST | https://www.google-ana |
| | 5186 | HTTP_STREAM_JOB | https://www.google-ana |
| | 5187 | URL_REQUEST | https://github.com/logi |
| | 5188 | DISK_CACHE_ENTRY | https://github.com/logi |
| | 5189 | HTTP_STREAM_JOB | https://github.com/ |
| | 5190 | CONNECT_JOB | ssl/github.com:443 |
| | 5191 | CONNECT_JOB | ssl/github.com:443 |
| ☑ | 5192 | SOCKET | ssl/github.com:443 |
| | 5193 | DISK_CACHE_ENTRY | https://assets-cdn.githu |
| | 5194 | DISK_CACHE_ENTRY | https://assets-cdn.githu |
| | 5195 | DISK_CACHE_ENTRY | https://assets-cdn.githu |
| | 5196 | DISK_CACHE_ENTRY | https://assets-cdn.githu |
| | 5197 | DISK_CACHE_ENTRY | https://assets-cdn.githu |
| | 5198 | DISK_CACHE_ENTRY | https://assets-cdn.githu |
| | 5199 | DISK_CACHE_ENTRY | https://assets-cdn.githu |
| | 5200 | DISK_CACHE_ENTRY | https://assets-cdn.githu |
| | 5201 | URL_REQUEST | https://collector.github |
| | 5202 | DISK_CACHE_ENTRY | https://collector.github |
| | 5203 | HTTP_STREAM_JOB | https://collector.github |
| | 5204 | UDP_SOCKET | [2001:4860:4860::8888] |
| | 5205 | URL_REQUEST | https://www.google-ana |
| | 5206 | DISK_CACHE_ENTRY | https://www.google-ana |
| | 5207 | HTTP_STREAM_JOB | https://www.google-ana |

```
                                dC5jb20vRGlnaUNlcnRIaWdoQXNzdXJhbmNlRVZSb290Q0EuY3JsM
                                MDQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwczovL3d3dy5ka
                                b20vQ1BTMB0GA1UdDgQWBBQ901Cl1qCt7vNKYApl0yHU+PjWDzAfB
                                gBSxPsNpA/i/RwHUmCYaCALvY2QrwzANBgkqhkiG9w0BAQsFAAOCA
                                hgLtxaDwNBx0wY12zIYKqPBKikLWP8ipTa18CK3mtlC4ohpNiAexK
                                4xFJcKx6HQGkyhE6V6t9VypAdP3THYUYUN9XR3WhfVUgLkc3UHKMf
                                2sPIoc4sUqIAY+tzunHISScjl2SFnjgOrWNoPLpSgVh5oywM395t6
                                1OG9d4Q3A84ytciagRpKkk47RpqF/oOi+Z6Mo8wNXrM9zwR4jxQUe
                                oVWNWlZopCJwqjyBcdmdqEU79OX2olHdx3ti6G8MdOu42vi/hw15U
                                8TUoE6smftX3eg==
                                -----END CERTIFICATE-----

t=132374 [st=  794]        SOCKET_BYTES_SENT
                           --> byte_count = 51
t=132379 [st=  799]        SIGNED_CERTIFICATE_TIMESTAMPS_RECEIVED
                           --> embedded_scts = "AWkAdgCkuQmQtBhYFIe7E6LMZ3AKPDWYBPkb37j
                           --> scts_from_ocsp_response = ""
                           --> scts_from_tls_extension = ""
t=132379 [st=  799]        SIGNED_CERTIFICATE_TIMESTAMPS_CHECKED
                           --> invalid_scts = []
                           --> unknown_logs_scts = []
                           --> verified_scts = [{"extensions":"","hash_algorithm":"SHA2
t=132379 [st=  799]        EV_CERT_CT_COMPLIANCE_CHECKED
                           --> certificate =
                                -----BEGIN CERTIFICATE-----
                                MIIHeTCCBmGgAwIBAgIQC/20CQrXteZAwwsWyVKaJzANBgkqhkiG9
                                MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwF
                                d3cuZGlnaWNlcnQuY29tMTQwMgYDVQQDEytEaWdpQ2VydCBTSEEyI
                                IFZhbGlkYXRpb24gU2VydmVyIENBMB4XDTE2MDMxMDAwMDAwMFoXD
                                MDAwMFowgf0xHTAbBgNVBA8MFFByaXZhdGUgT3JnYW5pemF0aW9uM
                                BAGCNzwCAQMTAlVTMRkwFwYLKwYBBAGCNzwCAQITCERlbGF3YXJlM
                                Ewc1MTU3NTUwMSQwIgYDVQQJExs4OCBDb2xpbiBQIEtlbGx5LCBKc
                                DjAMBgNVBBETBTk0MTA3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ
                                YTEWMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEVMBMGA1UEChMMR2l0S
                                MRMwEQYDVQQDEwpnaXRodWIuY29tMIIBIjANBgkqhkiG9w0BAQEFA
                                CgKCAQEA54hc8pZclxgcupjiA/F/OZGRwm/ZlucoQGTNTKmBEgNsr
                                bAvUaLP//T79Jc+1WXMpxMiz9PK6yZRRFuIo0d2bx423NA6hOL2RT
```

Was ist CT?

CT-Komponenten

Certificate Logs

**Vorteile und Mängel**

Zusammenfassung

# Vorteile von Certificate Transparency

- Schrittweiser Rollout
- Keine gravierende Änderungen
- Erweiterte Service-Angebote für CAs
- Flexibles und erweiterbares Framework

Was ist CT?

CT-Komponenten

Certificate Logs

**Vorteile und Mängel**

Zusammenfassung

# Mängel von Certificate Transparency

- CT verhindert die Ausstellung von gefälschten Zertifikaten nicht
- CT-Funktion von Google ist automatisch. Der Inhaber des SSL-Zertifikats  kann sie nicht ausschalten

Was ist CT?

CT-Komponenten

Certificate Logs

Vorteile und Mängel

**Zusammenfassung**

# Zusammenfassung

- CT stellt eine Sicherheitsfunktion dar, welche die Vertrauenswürdigkeit der Internetseiten steigert
- Chain-of-Trust-Modell wird durch Certificate Transparency nicht verändert (Fälschbarkeit bleibt)
- Stattdessen wird Chain-of-Trust Modell durch die Certificate Transparency erweitert mit einer “öffentlichen” Aufsicht und Kontrolle des gesamten TLS-Zertifikatssystem

# Quellen


- Google baut neuen Vertrauensraum für SSL-PKI auf, Arno Fiedler, Christoph Thiel, Datenschutz und Datensicherheit, Oktober 2014, Springer, Seiten: 680-683
- RFC 6962 – Certificate Transparency, Experimental Request for Comments, B.Laurie, A. Langley, E. Kasper, June 2013
- Public, verifiable, append-only logs, by Ben Laurie, October 2014, acmQueue
- Certificate Transparency (CT) - Alles was Sie wissen müssen, CertCenterAG, October 2014
- SSL Zertifikate und ihre Unterschiede, Kuketz IT-Security Blog, September 2012, https://www.kuketz-blog.de/ssl-zertifikate-und-ihre-unterschiede
- https://www.certificate-transparency.org