Certificate Transparency in Chrome

Questions: ct-policy@chromium.org
May 2016

This document details the criteria for a certificate to be considered CT Qualified.

In order to improve the security of Extended Validation (EV) certificates, Google Chrome requires that all certificates issued after 1 Jan 2015 be CT Qualified in order to be recognized as EV.

In order to improve the security of the Certificate Authority (CA) ecosystem, Google Chrome may require that certificates be considered CT Qualified in order to be recognized as trusted. This may be in response to security incidents, in which certificates from a particular CA are required to be CT Qualified in order to ensure compliance with stated policies and industry requirements. This may also be based on site operators signalling that certificates for a particular domain be CT Qualified in order to ensure transparency of the issued certificates.

Chrome's current Certificate Transparency implementation is as follows:

1. Google runs three geographically diverse CT logs which accept all certificates issued by CAs accepted by any major browser.
2. Google continues to invite other organisations to deploy CT logs in order to improve robustness.
3. On 1 Jan 2015 Chrome created a whitelist of certificates that contained EV policy OIDs included or pending inclusion in Chrome, that were logged in a qualifying log, and that would not qualify via SCTs embedded in the certificate (see below).
4. In March 2015 Chrome for desktop platforms ceased to show the EV indicator for certificates not in the whitelist and not CT qualified according to the criteria below.

Qualifying Logs

The criteria for qualifying logs can be found here.

Qualifying Certificate

A certificate is "CT qualified" if it meets one of the following criteria:

1. An SCT from a log qualified at the time of check is presented via the TLS extension OR is embedded within a stapled OCSP response;
   AND there is at least one SCT from a Google Log, qualified at the time of check, presented via any method;
   AND there is at least one SCT from a non-Google Log, qualified at time of check, presented via any method.
2. An Embedded SCT from a log qualified at the time of check is presented;
   AND there is at least one Embedded SCT from a Google Log, once or currently qualified;
   AND there is at least one Embedded SCT from a non-Google Log, once or currently

qualified;
AND there are Embedded SCTs from AT LEAST the number of logs once or currently qualified shown in Table 1.

“Once or currently qualified” means that the log was qualified or pending qualification at the time of certificate issuance, that the log was accepted prior to the time of check, but that the log may have been disqualified following acceptance, prior to the time of check.
“Embedded SCT” means an SCT delivered via an X.509v3 extension within the certificate.

Lifetime of certificate	Number of SCTs from distinct logs
<15 months	2
>= 15, <= 27 months	3
> 27, <= 39 months	4[1]
> 39 months	5

Table 1

Note that, so long as one of the above conditions is met by some combination of SCTs presented in the handshake, additional SCTs, regardless of the status of the SCT, will not affect the CT Qualification status positively or negatively.

Important note: many TLS servers do not support OCSP Stapling or the TLS extension, so CAs should be prepared to insert SCTs into issued EV certificates to maintain the EV indication.

Timeouts

The list of qualifying and once qualifying logs will be periodically refreshed during regular Chrome releases. If the installed version of Chrome has not applied security updates for a significant amount of time then CT checking will be disabled.

[1] EV certificates should never have a lifetime over 27 months.