Improving the Security of EV Certificates

Ben Laurie (benl@google.com)

May 2015

In order to improve the security of Extended Validation (EV) certificates, Google Chrome requires Certificate Transparency (CT) for all EV certificates issued after 1 Jan 2015.

Once we have gained experience with EV certificates we will publish a plan to bring CT to all 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 the TLS handshake it is presented in satisfies at least one of

1. At least the number of SCTs shown in Table 1, each from a log that is either qualified or pending qualification at time of certificate issuance, with all logs accepted as qualified prior to the TLS handshake, are embedded in the certificate, with at least one SCT being from a Google-operated log and at least one SCT being from a non-Google-operated log.
2. Two or more SCTs from qualifying logs[1] are embedded in a stapled OCSP response as specified in RFC 6962, with at least one SCT being from a Google-operated log and at least one SCT being from a non-Google-operated log.
3. Two or more SCTs from qualifying logs[2] are sent via the RFC 6962 TLS extension, with at least one SCT being from a Google-operated log and at least one SCT being from a non-Google-operated log.

[1] Note that in this case SCTs can be updated without modifying the certificate and are therefore expected to be from logs that are qualifying at the time of presentation.

[2] Note that in this case SCTs can be updated without modifying the certificate and are therefore expected to be from logs that are qualifying at the time of presentation.

And at least one SCT for the certificate validates and was issued by a log that is qualifying at the time of check.

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

Table 1

Note that, so long as the above conditions are met by some combination of SCTs presented in the handshake, additional SCTs, regardless of origin, are permitted.

Important note: most TLS servers do not support OCSP Stapling or the RFC 6962 TLS extension, so CAs should be prepared to insert SCTs into issued 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 and the client will cease to show EV indications.

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