Improving the Security of EV Certificates

All values in [] are TBD.

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

Once we have gained experience with EV certificates we will publish a plan to bring CT to all certificates.

We are pleased to announce the following plan.

1. Google is already running two geographically diverse pilot CT logs.
2. By March 2014 Google will deploy three geographically diverse production CT logs which will accept all certificates issued by CAs accepted by any major browser.
3. Google invites other organisations to deploy CT logs in order to improve robustness.
4. By March 2014 (Chrome release schedule permitting) Chrome will begin providing CT status information through the UI.
5. By July 2014 all EV certificates with validity periods beyond [July 2014] should be logged in at least [one] qualifying log (see below).
6. On 1 Jan 2015 Chrome will create a whitelist of valid EV certificates already issued without an embedded SCT [issued by CAs participating in CT] from all qualifying logs.
7. On or after (depending on Chrome release schedule) 1 Feb 2015 Chrome for desktop platforms will cease to show the EV indicator for certificates not in the whitelist and not CT qualified according to the criteria below. Chrome for mobile platforms will cease to show EV indicators for certificates that are not CT qualified according to the criteria below.

Qualifying Logs

A log is qualified if its URL, public key and Maximum Merge Delay (MMD) are known to and accepted by Chrome.

Chrome will accept a log's URL, public and MMD key if

1. The log has not been shown to have acted in bad faith.
2. The log is run by an entity believed to be capable of keeping the log up at least [99.9%] of the time.
3. The log has an MMD of no more than [24 hours].
4. The log conforms to RFC 6962.

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 from different qualifying logs [or logs that

once were qualifying] [operated by distinct entities][1] are embedded in the certificate.
2. [One][2] or more SCTs are embedded in a stapled OCSP response as specified in RFC 6962.
3. [One][3] or more SCTs are sent via the RFC 6962 TLS extension.

And at least one SCT for the certificate validates and was issued by a qualifying log.

Lifetime of certificate	Number of SCTs
<15 months	2
15 - 27 months	3
27 - 39 months	4
> 39 months	N/A[4]

Table 1

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 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.

Google will keep an authoritative list of qualifying logs and post changes to that list on the public CA/B Forum mailing list and on chromium.org.

[1] This can clearly only apply if at least [two] distinct entities actually run logs.
[2] It is possible to accept a single SCT because CAs can get new SCTs as needed and present them in OCSP, however if that does not happen in practice the limit will need to be higher.
[3] This low limit will only be possible if server s/w automatically renews SCTs. If manual intervention is required, a higher limit will be necessary.
[4] No such certificates should exist.