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 [date TBD].

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

We are soliciting feedback on the following plan.

1. Google is already running a pilot CT log.
2. By Dec 2013 Google will deploy three geographically diverse production CT logs which will accept all certificates issued by CAs accepted by any major browser (which are [Chrome, Internet Explorer versions [?], Safari, Firefox and Opera]).
3. Google invites other organisations to deploy CT logs in order to improve robustness.
4. On [date TBD] Chrome will begin providing CT status information through the UI.
5. By [date TBD] all EV certificates with validity periods beyond [date TBD] should be logged in at least [one] qualifying log (see below).
6. On [date TBD] 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 [date TBD] Chrome will cease to show the EV indicator for certificates not in the whitelist and 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. [Three] or more SCTs 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.

Timeouts

Chrome will regularly synchronise its list of qualifying logs with Google's servers. If the last successful synchronisation was more than [10 weeks] ago, the client will [stop checking CT] and [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.

[1] This can clearly only apply if [three] 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.