Expect-CT

Emily Stark
estark@chromium.org
IETF 97

Background

Certificate Transparency (CT): a framework for publicly logging certificates and proving that they've been logged. Standardization in TRANS WG.

Background

Today, domain owners can monitor logs for misissued certificates... but how do they defend against unlogged misissuances?

Expect-CT

Allow site owners to opt in to CT enforcement in the browser.

Expect-CT

```
HTTP/1.1 200 OK

...

Expect-CT: require; report-uri="https://..."; max-age: 31536000
```

Asks the browser to refuse and report connections that violate the browser's CT policy (e.g. two Signed Certificate Timestamps from two different logs).

Expect-CT

```
HTTP/1.1 200 OK

...

Expect-CT: report; report-uri="https://..."; max-age: 31536000
```

Allows the site owner to discover misconfigurations before turning on enforcement.

Expect-CT

- HTTP header for deployability.
- Syntax/semantics familiar to site operators (from HSTS).
- Allows site operators to ensure that all certificates in use for their domains are publicly logged.

Next steps

- Draft at https://github.com/bifurcation/expect-ct
- Up for adoption!