First Issued

Phillip Hallam-Baker

Origins

- Proposal for 3 Day certificates (2005 on)
  - "Age of certificate is useful"
    - Older certificates are evidence of longevity
- Solution
  - "Member since" extension

Why now?

- Short lived certificates
- User accessible safety information
  - Users are familiar with ‘established 1977’
- Safe Browser project

Objections

- We own the browser
  - Only the largest browsers get to decide the future.
- ‘PKIX doesn’t work’
- The information is in CT
  - Not in a form users can understand
  - Requires additional CT processing
    - Would have to specify to be useful

Charter text

- Examine requirements and if appropriate define a First-Issued certificate extension.

Certificate age provides an indication of trustworthiness of the certificate subject in a format that is familiar to end users (c.f. ‘Established’). Providing this information in a Certificate allows it to be used as part of a basis for proactive browser security measures.

Milestone: RFC June 2018