CAA

Phillip Hallam-Baker, Rob Stradling
Ben Laurie
Objectives

1. Allow CAs to avoid certificate mis-issue
2. Enable applications to enforce restrictions

3. Deploy (1) really, really quickly
   - Weeks
   - Cost of mis-issue is very, very large
Use Case

• Domain example.com decides
  – Only Carol CA can issue certs as external CA

• Publishes DNS record:
  – example.com CAA 1 policy 1.3.6.1.4.35405.666.1

• Carol CA receives cert request
  – Applies auth criteria and issues if passes

• Other CS receives cert request
  – Rejects request
CAA + DANE

- CAA is not DANE
  - Does not depend on DNSSEC (but it helps)
  - Does not require client code (but it is experience)

- If DANE extended to support issue restrictions
  - CAs would likely be required to support BOTH
  - Long term consequences limited to CAs
Timeline

2011-05  Begin deployment at CAs
2011-08  Technical feedback
2011-12  Propose to CABForum as requirement
2012-04  Publish as Criteria Requirement
[2013-04  Criteria Requirement Active]
[2014-06  Old WebTrust Audits Expire]