Decoupling Deployment in CT

Phillip Hallam-Baker
Comodo Group Inc.
Problem

1. Getting buy in from CAs is multi-step
   1. Get buy-in 'in principle' to disclosing customers
   2. Get buy-in to implement code
   3. Get buy-in to deploy

- Problem
  - May be delay of several years between 1 and 2
  - Personnel may change over time
  - Need to get buy in again
Multi-Party Disclosure

- I will show you mine
  - If you (eventually) show me yours

- Disclosing customer lists is a business cost
  - Must be matched by a business advantage
Proposed Solution (Simple)

- Participating CAs publish list of issued certs
  - Simple format (JSON)
  - Signed but
- Get delivery on publication commitment ASAP
  - Commitment to code becomes easier
Advanced Solution

- Anyone can publish cert lists
  - EFF, Netcraft, Other CAs
- CAs can measure cost of disclosure
  - (Probably) rather small
  - Make case to commit
- Explore selective disclosure possibilities
  - Mark some intermediaries for disclosure or not.