Three Minor Fixes

Phillip Hallam-Baker
VeriSign Inc.
Security Usability
Member since

• What information do we have today that might provide value to relying parties?
  – Date that subject first obtained a certificate
  – In the database
  – Can be put into the certificate at low cost
Community Name

• LOGOTYPE Extension
  – Subject
  – Issuer
  – List (Community)

• Accessibility
  – Must work in voice, Braille browser etc.
  – We have X.500 DN for Subject, Issuer
  – Need analog for Community Logos
Security Indicator Suppression

- Device based Certs
- Authentication: Negligible
- WebTrust Compliant: Yes (!)
- Requirement: work with any browser

- Solution:
  - OID states that security representations are made to infrastructure, not user