Revocation

Phillip HallamBaker

What are the dimensions?

- Rule 81 Applies
  - There are no stupid questions
  - Because there are some *very* stupid implementations
  - Have to ‘unlearn’ PKIX

Views

- Certificate Authorities
  - Issue Certificates, CRL, OCSP
- Subject applications
  - Do they provide any revocation data?
- Relying Parties
  - How do applications handle revocation?

Revocation Mechanisms

- CRL
- OCSP

End Entity Certificates

- Distribution Points
  - What happens if there is more than one?

OCSP Modes

- Reporting from a CRL
  - Only knows the bad certificates
    - Reports ‘GOOD’ for certificate that never existed
- Reporting from a status database
  - Knows good and bad certificates
    - Can say ‘this never existed’

OCSP Signing Certificate

- What trust anchors are accepted
  - Can Comodo report status for Symantec cert?
- What Key usage bits are set
- What EKUs
- What Policy OIDs

TLS Stapling

- In scope or not?

OCSP Processing

- Hard fail or not?

What did I miss?