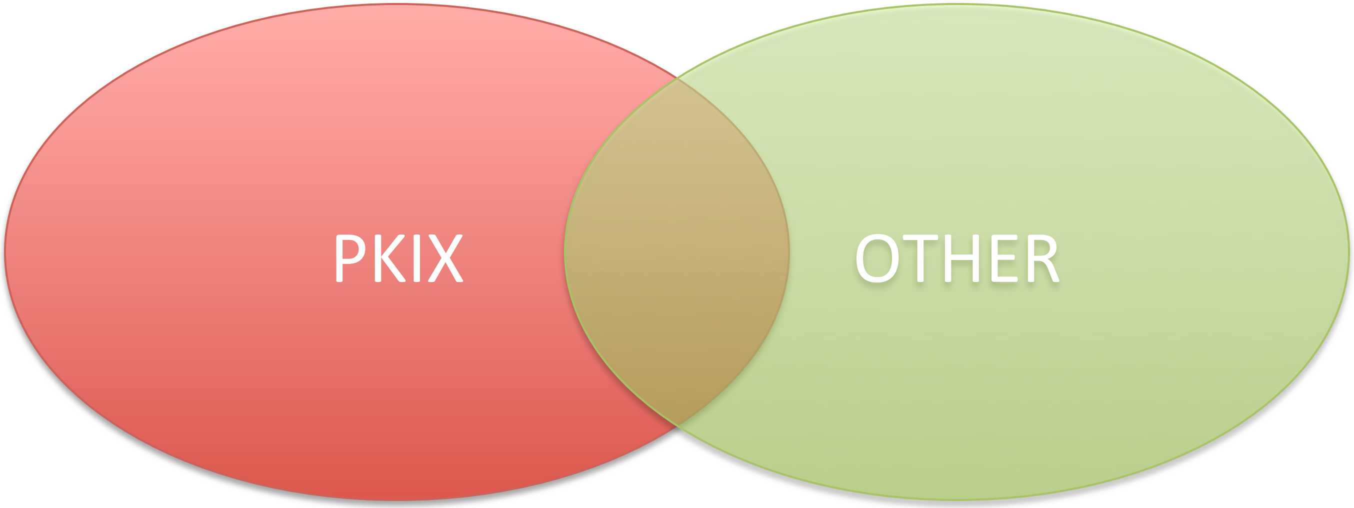
Revocation in WebPKI

Phill Hallam-Baker

Comodo

Standards intersection



PKIX but not RFC5280

- Semantics of Revocation Reasons
  - Says what tag to use
  - Not what tag means or when to use it
  - [X.509 spec has definitions]

Servers

- Is OCSP stapling supported?
  - Yes (Apache, IIS, LiteSpeed, ngnix)
- [Is OCSP stapling on by default?]
- [Does server check cert status regularly?]
- [Are frequent certificate updates supported?]

Clients

- Supported Revocation Checking Mechanisms
  - CRL / OCSP?
- User Experience for Certificate Status Invalid?
- User Experience for Certificate Status Valid?
- What sources are trusted to sign CRLs or OCSP responses?
- Does this vary for DV/EV?