Field / Extension Certificate Processing (Non-Revocation)

Ben Wilson, DigiCert

Excluded from this Scope

Revocation Related Mechanisms

- Blacklisting
- OCSP Stapling
- Revocation-related Configurations

Lesser-Used Capabilities

- Issuer alternative name / Subject info access
- Subject directory attribute
- Policy constraints / inhibit any policy
- Client Authentication TLS

To Be Added

- More Analysis of the Trust Model
- Consistency/divergence with historic PKIX
- More on browser behavior / Survey Table
- More on Security-Related Issues and Protocol Vulnerabilities
- Effectiveness of warnings and dialog boxes
- Mobile platform capabilities / behaviors

Where do We Go from Here

Tasks

- We need a better baseline description of the Web PKI and then review by more experts
- Insert contributions from broader group

Ultimate Mission:

Have a meaningful influence on User Agents and Harmonize Web PKI UA behaviors to improve experience and security of end users