# wpkops WG Charter Review

IETF 86 Orlando

March 2013

# WG Goal

- Describe how the Web PKI "actually" works in the set of browsers and servers that are in common use today
- To that end, the working group will document current and historic browser and server behavior, including
  - The trust model on which it is based
  - The contents and processing of fields and extensions
  - The processing of the various revocation schemes
  - How the TLS stack deals with PKI
  - The state changes that are visible to and/or controlled by the user
  - Identification of when Web PKI mechanisms are reused by other applications and implications of that reuse

# Constraints

- Where appropriate, specific products and specific versions of those products will be identified, but recording the design details of the user interfaces of specific products is not necessary
- Only server-authentication behavior encountered in more than 0.1 percent of connections made by desktop and mobile browsers is to be considered
  - While it is not intended to apply the threshold with any precision, it will be used to justify the inclusion or exclusion of a technique

# Outside Scope

- Describe how the Web PKI "should" work
- Examine the certification practices of certificate issuers
- Investigate applications (such as client authentication, document signing, code signing, and email) that often use the same trust anchors and certificate processing mechanisms as those used for Web server authentication

# Document Milestones

| **Document** | **1st WG draft** | **IESG submission** |
|---|---|---|
| Trust Model | June 2013 | June 2014 |
| TLS Stack Operation | Oct 2013 | June 2014 |
| Certificate Revocation | Oct 2013 | Oct 2014 |
| Field and Extension Processing for Certificates, CRLs and OCSP responses | Feb 2014 | Feb 2015 |