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

<table>
<thead>
<tr>
<th>Document</th>
<th>1st WG draft</th>
<th>IESG submission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Model</td>
<td>June 2013</td>
<td>June 2014</td>
</tr>
<tr>
<td>TLS Stack Operation</td>
<td>Oct 2013</td>
<td>June 2014</td>
</tr>
<tr>
<td>Field and Extension Processing for Certificates, CRLs and OCSP responses</td>
<td>Feb 2014</td>
<td>Feb 2015</td>
</tr>
</tbody>
</table>