• Assign Minute taker (start recording)
• Roll call
• Antitrust Statement
• Goals and Progress
• Subscriber Keys
• Signing Service
• Parking Lot Items
• Other Items
• Next Meeting
Goals and Progress

- Merge non-EV and EV requirements - DONE
- Rationalize EV requirements - DONE
- Address move to 4096-bit RSA - DONE
- Cleanup and clarify requirements - DONE
- Update Subscriber Private Key Protection requirements
- Update Signing Service requirements
- Move CSBR to Pandoc/RFC 3647 format – Update in draft
- CSBR less dependent on SSL BRs and SSL EVGs
• Key generation performed on a crypto module
• Crypto module may be operated by the Subscriber, Cloud Provider or Signing Service
• CA must verify the key was generated on a crypto module, for example
  • CA ships HSM with preinstalled key pair
  • CA provides Signing Service
  • Subscriber provides certificate request over hardware crypto service provider (CSP)
  • Subscriber uses HSM key attestation
  • Subscriber provides report of cloud key protection solution
Signing Service Requirements

• Does not import private keys
• Secure authentication to allow Subscriber to generate the key pair or activate the private key for signing
• Logs all access, operations and configuration on the private key itself
• Logs must be available to the Subscriber
• Audit – Are these required? CSBR, NetSec, WebTrust for CA, and ETSI audits
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Owner</th>
<th>Priority</th>
<th>Comments</th>
<th>Ballot</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Subscriber private key protection should be updated. Cloud-based key protection should be considered.</td>
<td>Ian</td>
<td>1</td>
<td>Presented on 6/18/20. Recommend removing CC and adding eIDAS. Outcome is that the reqts for keys would be the same for EV and non EV. Ian to propose language.</td>
<td>CSC-6</td>
</tr>
<tr>
<td>7.2</td>
<td>Signing Service warranties should be separated from the CA warranties</td>
<td>Bruce/Ian</td>
<td>1</td>
<td>Will be address in Signing Service update ballot</td>
<td></td>
</tr>
<tr>
<td>13.2.1</td>
<td>Invalidity Date</td>
<td>Corey</td>
<td>1</td>
<td>Windows does not support Invalidity Date. Ballot to provide clarrification in CSBRs.</td>
<td></td>
</tr>
<tr>
<td>All</td>
<td>Move CSBRs to RFC 3647 format and into pandoc format</td>
<td>Corey</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.1.1</td>
<td>Refers to non-EV CS certificates, has a requirement for additional validation for companies less than three years old (we've discussed this recently), but this requirement is missing for EV code signing certificates.</td>
<td>Tim H</td>
<td>2</td>
<td>Ballot to resolve that non-EV requirement is higher tha EV requirement</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SSL BR and SSL EV Guidelines versions</td>
<td>Bruce</td>
<td>2</td>
<td>Need plan to update CSBRs with latest acceptable versions of the SSL BR/EVGs</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Certificate suspension</td>
<td>Dimitris</td>
<td>2</td>
<td>Reference to SSL BRs may make the requirement about certificate suspension unclear. Could be resolved with a ballot indicating that certificate suspension is not allowed</td>
<td></td>
</tr>
<tr>
<td>11.5</td>
<td>High risk certificate requests should either be removed or updated to provide common methods for all CAs.</td>
<td>Ian</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.2.1</td>
<td>CSBR 9.2.1 states “No stipulation”. Update CSBRs to ensure SAN is not allowed.</td>
<td>Tim H</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.2.</td>
<td>Email address in subject DN</td>
<td>Tim H</td>
<td>2</td>
<td>Brought up by Microsoft rep at virtual F2F. Hard to get EV for these entities. Is there another way? Need separate meeting to brainstorm. Many open-source people need these.</td>
<td></td>
</tr>
<tr>
<td>11.1.2</td>
<td>How to identify individuals working on open source code as part of a consortium?</td>
<td>Ian</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.2.4</td>
<td>Should we address including givenName and surName in certificates?</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Other items
Next Meeting

• Thursday, 21 October 2021, 12:00 ET
Thank you