 Mozilla Root Program Update for the CA/Browser Forum Ottawa - February 2023

Link to Previous Mozilla Face-to-Face Briefing (October 2022)

Ben Wilson and Kathleen Wilson
Mozilla Root Store Program Managers
Outline

- Recap of Changes in Mozilla Root Store Policy (version 2.8.1)
- Upcoming Changes and Discussion Items for MRSP version 2.9
- Root Inclusion Considerations
- CA Inclusion Requests
- New Whiteboard Labels for Compliance Incidents
- Currently-Open CA Compliance Incidents
- Analysis of Past CA Incident Types
- Mozilla’s Top Priorities and Goals
Recap: MRSP v2.8.1

Certification Authorities must follow and be aware of discussions in both
- the Mozilla dev-security-policy forum, and
- the CCADB Public List

Certificate Policies (CPs), Certification Practice Statements (CPSes), and combined CP/CPSes MUST:
- clearly explain Domain Validation procedures and indicate applicable BR § 3.2.2.4 subsections
- be updated at least every 365 days
- be maintained from creation of CA until CA hierarchies are no longer trusted by the Mozilla root store
  - if CA certificates were included by Mozilla before December 31, 2022, then the CA must still maintain links for “reasonably available historic versions”

JSON Arrays of Partitioned CRLs must
- contain a critical Issuing Distribution Point extension
- have the URI derived from either: the URI as encoded in the distributionPoint field of an issued certificate’s CDP (RFC 5280, § 5.2.5), or the URL in the "JSON Array of Partitioned CRLs" field in the CCADB
Upcoming changes: MRSP v. 2.9

https://github.com/mozilla/pkipolicy/labels/2.9

Require CA operators to submit Compliance Self-Assessments annually
Mozilla GitHub Issue # 240
https://wiki.mozilla.org/CA/Compliance_Self-Assessment

Clarify requirements for reporting security incidents affecting CA systems
Mozilla GitHub Issue # 252

Adopt S/MIME Baseline Requirements
Mozilla GitHub Issue # 258

Establish limits on the useful life of Root CA Certificates
Mozilla GitHub Issue # 232;
https://wiki.mozilla.org/CA/Root_CA_Lifecycles
Transition to 15-year Root CAs

<table>
<thead>
<tr>
<th>Key Material Created</th>
<th>Removal of Websites Trust Bit</th>
<th>Distrust for S/MIME After Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before 2006</td>
<td>April 15, 2025</td>
<td>April 15, 2028</td>
</tr>
<tr>
<td>2006-2007</td>
<td>April 15, 2026</td>
<td>April 15, 2029</td>
</tr>
<tr>
<td>2008-2009</td>
<td>April 15, 2027</td>
<td>April 15, 2030</td>
</tr>
<tr>
<td>2010-2011</td>
<td>April 15, 2028</td>
<td>April 15, 2031</td>
</tr>
<tr>
<td>2012- April 14, 2014</td>
<td>April 15, 2029</td>
<td>April 15, 2032</td>
</tr>
<tr>
<td>April 15, 2014 - present</td>
<td>15 years from creation</td>
<td>18 years from creation</td>
</tr>
</tbody>
</table>

**Distrust Date**

For TLS: Websites trust bit will be removed 15 years after CA key creation.
For Email: Mozilla will set “Distrust for S/MIME After Date” to 18 years from CA key creation.

**CA Key Creation**

Will be determined by date in auditor-witnessed key generation report.
To be Discussed for MRSP v.2.9

- #250 Clarify MRSP § 5.3.2 to expressly require CCADB reporting of revoked CA certificates
- #241 Revisit and improve MRSP § 8.4 Technically-Constrained Sub-CAs
- #237 Require more detail in CPSes about CA ownership and control (operations, security, sources of funding, liability, etc.)
- #214 Clarify OCSP/CRL Availability Requirements
Root Inclusion Considerations

Goal: Help us make earlier, more objective decisions.

Unacceptable Behavior
Mozilla should deny root inclusion request.

Concerning Behavior
In aggregate may lead to denying the root inclusion request.

Warning Signs
CA operators must improve their operations and demonstrate their ability to maintain the higher level of operations, or their root inclusion request will be denied.

Please review https://wiki.mozilla.org/CA/Root_Inclusion_Considerations, and provide feedback on the Mozilla dev-security-policy list.
<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Received - Initial Status</strong></td>
<td>12</td>
</tr>
<tr>
<td>CA hasn’t provided enough information to begin review process</td>
<td></td>
</tr>
<tr>
<td><strong>Information Verification</strong></td>
<td>19</td>
</tr>
<tr>
<td>CA is providing additional information, which is being reviewed</td>
<td></td>
</tr>
<tr>
<td><strong>Ready for CP/CPS Review and Public Discussion</strong></td>
<td>2</td>
</tr>
<tr>
<td>CA’s CP and CPS are being reviewed and updated</td>
<td></td>
</tr>
<tr>
<td><strong>In Public Discussion</strong></td>
<td>2</td>
</tr>
<tr>
<td>CA is in period of public review and comment</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>35</td>
</tr>
</tbody>
</table>

https://wiki.mozilla.org/CA/Dashboard
Whiteboard Labels

  mis-issuance of a certificate (CA, DV, OV or EV respectively)

- `[crl-failure]` / `[ocsp-failure]` failure to provide certificate status; malformed or expired CRL or OCSP, respectively

- `[policy-failure]` failure to update CP/CPS annually, failure to comply with practice in CP/CPS, misunderstanding requirements, failed implementation

- `[disclosure-failure]` failure to disclose an ICA, failure to report revocation of an ICA, non-disclosure of EV sources, miscommunication, poor communication, etc.

- `[audit-failure]` failure to: perform an audit, include ICA in audit, upload audits to CCADB

- `[audit-finding]` a non-conformity or qualified opinion from an audit report

- `[ca-revocation-delay]` / `[leaf-revocation-delay]` delayed revocation of a CA / leaf certificate

- `[uncategorized]` or just `[ca-compliance]` for anything not listed above
## Currently Open Compliance Incidents

[https://wiki.mozilla.org/CA/Incident_Dashboard](https://wiki.mozilla.org/CA/Incident_Dashboard)

<table>
<thead>
<tr>
<th>Types of Incident</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>OV Misissuance</td>
<td>7</td>
</tr>
<tr>
<td>EV Misissuance</td>
<td>7</td>
</tr>
<tr>
<td>CRL Failure / OCSP Failure</td>
<td>5</td>
</tr>
<tr>
<td>CA Misissuance</td>
<td>4</td>
</tr>
<tr>
<td>Disclosure Failure</td>
<td>3</td>
</tr>
<tr>
<td>CA Revocation Delay</td>
<td>3</td>
</tr>
<tr>
<td>Leaf Revocation Delay</td>
<td>3</td>
</tr>
<tr>
<td>DV Misissuance</td>
<td>2</td>
</tr>
<tr>
<td>Uncategorized</td>
<td>1</td>
</tr>
</tbody>
</table>
~ 1,000 Incidents, 2015-2023, by Type

- CA Misissuance - 46 | 5%
- DV Misissuance - 94 | 9%
- OV Misissuance - 308 | 30%
- EV Misissuance - 157 | 16%
- Disclosure Failures - 64 | 6%
- Policy Failure - 42 | 4%
- Revocation Delays - 103 | 10%
- CRL/OCSP Failure - 128 | 13%
- Audit Finding - 27 | 3%
- Uncategorized - 41 | 4%

https://wiki.mozilla.org/CA/Bug_Triage#Compliance_Problems_and_Incidents
Mozilla’s Top Priorities and Goals

#1 - Keep the web safe for our end users
       A fast and secure TLS handshake with a browser URL bar that is easy for end users to understand.

Public-facing and transparent processes
       Use knowledge from the community in policy adoption, root inclusion, and problem resolution. Continue to update the BRs, policies, and practices as web attack scenarios continue to advance.

Consistent requirements and enforcement for CAs across the globe
       Vet CAs and monitor them to ensure they do not expose users to risk. Share knowledge to prevent repeating mistakes.

Continue to improve automated monitoring and reporting abilities
       Faster identification and resolution of problems. More timely inclusion of root CA certificates based on program priorities.

Hard-fail for revoked TLS certificates without leaking browsing information
       CRLite, Requiring full CRL information, Revocation Reason Codes – policy/consistency
Contacting Us:
certificates@mozilla.org