Microsoft Trusted Root Program Update
CA/Browser Forum
Face to Face Meeting 47 Thessaloniki
June 12, 2019
Agenda

- Intro of Microsoft Attendees
- Program Communications
- Microsoft Root Change Terminology
- Program Updates
- Microsoft Edge and Chromium Open Source
Program Communications Reminders

• msroot@microsoft.com should be used for communications to ensure timely response

• Program requirements can be found on Microsoft Docs (https://docs.microsoft.com/en-us/) at: https://aka.ms/RootCert

• Program audit requirements can be found on Microsoft Docs at: https://aka.ms/auditreqs
## Microsoft Root Change Terminology

<table>
<thead>
<tr>
<th>Disallow</th>
<th>Designed for major security incidents. Certificates added to the Disallowed list can be issuing or leaf certificates and DO NOT need to be in the Certificate Trust List (CTL). Disallowed certificates are blocked from being trusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removal</td>
<td>Removal of root from the Certificate Trust List. All certificates no longer trusted</td>
</tr>
<tr>
<td>Disable</td>
<td>Introduced in Windows10RS1. Disables all certificates issued by the root certificate except for Code Signing and Time Stamping. Code Signing and Time Stamping certificates will continue to be trusted if the certificate was issued prior to the Disable date</td>
</tr>
<tr>
<td>NotBefore</td>
<td>Introduced in Windows10RS2. Allows granular disabling of a root certificate or specified EKU capabilities of a root certificate. The NotBefore property distrusts the certificate or specified EKU if it was issued after the NotBefore date. Certificates issued prior to the NotBefore date will not be impacted</td>
</tr>
</tbody>
</table>
Program Updates

- Root Store Certificate Trust List (CTL) updated monthly (except December)
  - Additions and non-deprecating modifications will be completed any month
  - CA-initiated and CA-confirmed deprecations will occur on even numbered months (e.g. Feb, Apr, Jun, Aug, Oct)
  - Microsoft-initiated deprecations will occur in February and August releases

- Plan to publicly share backlog of pending root store changes starting by July (preview in next slide)

- Initiated vetting of all new CA applicants and will review existing CAs at least annually. Includes:
  - Beneficial Ownership Screening
  - Anti-Corruption
  - Business Verification
  - Trade Sanctions
  - Other due diligence as appropriate
Upcoming Changes Backlog Preview

- Allows certificate users who have active certificates chaining up to a deprecating root to be made aware of changes that may impact their certificates.

- Update packages will be available for download and testing at https://aka.ms/CTLDownload.
Microsoft Edge and Chromium Open Source

- We will adopt Chromium as the web platform for Microsoft Edge
- We intend to become a significant contributor to Chromium
- Microsoft Edge will be delivered and updated for all supported versions of Windows and on a more frequent cadence
- Preview builds are available for insight into our testing and contributions. Feedback is encouraged. Go to: https://www.microsoftedgeinsider.com/