Microsoft

Microsoft Trusted Root Program Update

CA/Browser Forum
Face to Face Meeting 46 Cupertino
March 13, 2019

Agenda

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

Program Communications

- 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

Removal	Removal of root from the Certificate Trust List (CTL). All certificates no longer trusted
Disable	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
NotBefore	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

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
  - Microsoft-initiated deprecations will occur in February and August releases
- Publicly sharing pending root store changes (our backlog)
- Continued end-to-end examination of each root in the root store for EKUs, use, contract compliance and other issues which may represent risk to Microsoft customers
- Continued efforts toward automation of program processes to minimize errors and enable increased verification of program compliance
- The standard code-signing is required for all CAs who issue code-signing certificates. EV Code-signing audits do not require the standard code-signing audits
- Reminder: We have deprecated the practice of cross-signing roots to enable kernel code signing. Current cross-signed roots WILL NOT be renewed nor re-cross signed

Microsoft Edge and Chromium Open Source: Our Intent

- We will adopt Chromium as the web platform for Microsoft Edge desktop
- We hope and intend to become a significant contributor to Chromium, in a way that can make not just Microsoft Edge—but other browsers as well—better on both PCs and other devices
  - Initial areas of focus include ARM64 support, Accessibility, PC-hardware evolution (e.g. touch) and security
- Microsoft Edge will be delivered and updated for all supported versions of Windows and on a more frequent cadence
- We invite you to join our community by installing preview builds when they're available and staying current on our testing and contributions