Microsoft

Microsoft Trusted Root Program Update

CA/Browser Forum
Face to Face Meeting 48 Guangzhou, China
November 5-7, 2019

Agenda

- Intro of Microsoft Attendees
- Program Communications
- Program Operating Principles
- General Approach to Adding CAs/Roots
- Program Updates
- Microsoft Edge Browser Update

Program Communications Reminders

- msroot@microsoft.com should be used for communications to ensure timely response
- Program requirements can be found on Microsoft Docs at: https://aka.ms/RootCert
- Program audit requirements can be found on Microsoft Docs at: https://aka.ms/auditreqs

Root Program Operating Principles

- Our Program reflects Microsoft's values. We should be able to stand by the statement *"Microsoft runs on trust and Microsoft trusts <Company name> Certificate Authority and the certificates they issue to ensure the security and privacy of our customers"*
- We run a reliable, secure root store for the benefit of our users. Security of our users is paramount
- Our root store provides a consistent user experience across our products and services
- All CAs are treated equally, independent of their geographic area of operations or market size. Same rules for everyone, rigorously enforced
- Trust, but verify through audits (WebTrust and ETSI) and available open source and proprietary PKI monitoring
- Service and encourage the widest possible use of PKI activities
- CAs are partners in the certificate lifecycle, audits, ecosystem monitoring and security response
- Microsoft independently conducts regular risk assessments to inform our "trust" decisions

General Approach to Adding New CAs/Roots

- Application completed
- Certificate Policy/Certificate Practice Statement (CP/CPS) review
- Review of audit reports
  - Auditor certified by either WebTrust or EU governance bodies?
  - Any qualifications from the audit?
  - Test websites active?
- Telemetry
- Vetting of the entity (CA and related businesses)
  - Management
  - Operations
  - Beneficial Ownership Screening
  - State-Owned Entity review
  - Other due diligence as appropriate
- Threat and intelligence review
- Legal review and contractual agreement
- Microsoft leadership approval
- Annual review of all the above while under contract

Program Updates

- Root Store Certificate Trust List (CTL) updated monthly (except December)
- Publicly share backlog of pending root store changes which allows certificate users who have active certificates chaining up to a deprecating root to be made aware of changes that may impact their certificates
  - Release notes at https://docs.microsoft.com/en-us/security/trusted-root/release-notes
  - October release notes released in xml format (link)
- Update packages will be available for download and testing at https://aka.ms/CTLDownload
- Updating/Cleanup of our program requirements:
  - Separating out application requirements and incident requirements into stand alone documents
  - Removing outdated timelines for various changes
  - Partnering with other Certificate Consumers on "Aligning the BRs with existing Browser Requirements"
    - https://github.com/cabforum/documents/compare/master...sleevi:2019-10-Browser_Alignment

Microsoft Edge Updates

- Details on Windows Blog: https://blogs.windows.com/windowsexperience/2019/11/04/introducing-the-new-microsoft-edge-and-bing/
- The release candidate can be downloaded now with general availability targeting January 15 in more than 90 languages
- Microsoft Edge runs on the same Chromium web engine as Google's Chrome browser, offering best in class web compatibility and performance
- A new tracking prevention default in Microsoft Edge. Starts with tracking prevention on by default for a more private browsing experience
- With SmartScreen and Tracking prevention, Edge helps protect users from phishing schemes, malicious software and new types of malware like cryptojacking
- Microsoft Edge now offers new InPrivate mode across the entire web experience so online searches and browsing are not attributed to the user, offering more control over personal data