

Microsoft Trusted Root Program Update

CA/Browser Forum

Face to Face Meeting 49 Bratislava, Slovakia

February 18-20, 2020



Agenda

- Introduction of Microsoft attendees
- Communications reminders
- Change management
- Requirements updates
- ECU updates
- Kernel mode code signing update
- 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>

Change Management

- 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>
- Update packages will be available for download and testing at <https://aka.ms/CTLDownload>

Program Requirements Update

- Updated requirements have been posted: <https://Aka.ms/rootcert>
- Key Highlights:
 - New CA application procedures and incident response procedures updated, have their own pages
 - CAs are required to have at least one 24/7-monitored contact or alias meant for incident management.
 - Reason Code must be included in revocations. CAs must update the CCADB when revoking any intermediate certificates within 30 days.
 - Program Participants must keep hierarchy information accurate in the CCADB when changes occur
 - Other changes include updates to language and structure of the document

EKU Updates

- IPsec EUs, Encrypting File Systems are now deprecated and will be removed from CAs in future releases
- Code signing audits are required from all CAs who have the EKU. We will remove the EKU from any non-compliant CAs starting in the April release.

Kernel Mode Code Signing (KMCS) Update

- Certs for KMCS must expire by July 1st, 2021
 - Effective for KMCS certs issued AFTER Jan 20th, 2020
 - This policy DOES NOT apply to KMCS-enabled certificates that will be used for regular codesigning only
- FAQ for developers found here:
 - <https://docs.microsoft.com/en-us/windows-hardware/drivers/install/deprecation-of-software-publisher-certificates-and-commercial-release-certificates>

Edge (Anaheim) Update

Officially launched new Edge browser (Anaheim) on January 15