Microsoft

Microsoft Trusted Root Program Update

CA/Browser Forum
Face to Face Meeting 52 (Virtual)
March 2-4, 2021

Agenda

- Change management
- Program Requirements update
- Testing
- ALV extended
- Communications reminder
- Kernel mode code signing update

Change Management

- Root Store Certificate Trust List (CTL) updated monthly (except December)
  - Update packages will be available for download and testing at https://aka.ms/CTLDownload - Please confirm testing when asked!
- 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 are posted once testing link is live.
  - Release notes at https://docs.microsoft.com/en-us/security/trusted-root/release-notes

Program Requirements Update

- Current requirements are posted at: https://Aka.ms/rootcert
- We will be reviewing program requirements in June 2021 for potential updates. Any updates will be emailed with information
  - If there is any confusion on any current requirements in our program, please email us at msroot@Microsoft.com.

Program Requirements Update cont.

- New pages with procedures for testing and deprecation definitions have been posted. There is no new update to the procedures, but information is posted for reference.
- New pages can be here: Testing - Microsoft Trusted Root Certificate Program | Microsoft Docs and here: Deprecation Actions - Microsoft Trusted Root Certificate Program | Microsoft Docs

Program Requirements Update cont.

- Formalization for ETSI audit requirements
  - Current: All CAs must be audited against the CA/Browser Forum requirements and compliance to these requirements must be stated in the audit letter. ACAB'c [https://acab-c.com] has provided guidance that meets the Microsoft requirements.
  - Link to ACAB'c audit attestation letter are here: https://www.acab-c.com/downloads/

Program Requirements Update cont.

- Reversion to previous section 3.A.8 requirements
  - Current: Issuing CA certificates that chain to a participating Root CA must separate Server Authentication, S/MIME, Code Signing, and Time Stamping uses. This means that a single Issuing CA must not combine server authentication with S/MIME, code signing or time stamping EKU. A separate intermediate must be used for each use case.
  - Previous: Issuing CA certificates that chain to a participating Root CA must be constrained to a single EKU (e.g., separate Server Authentication, S/MIME, Code Signing, and Time Stamping uses. This means that a single Issuing CA must not combine server authentication with S/MIME, code signing or time stamping EKU. A separate intermediate must be used for each use case.

Testing

- All CAs currently can test changes roughly two weeks before the changes release.
- If your CA has changes in a release, you will be notified about testing once the test changes are live. We ask that you test the changes within 5 business days of notice and confirm that certificates are working or not working as expected.

ALV extended to full CA hierarchy

- Microsoft will now be reviewing audit statements for the full hierarchy. This includes the root certificate and intermediate certificates that reported in the CCADB
- We will be reviewing compliance using ALV for both TLS audits and Code Signing audits.
- Microsoft will be reaching out to CAs that are non-compliant during the upcoming months to allow CAs to remediate issues prior to taking action.

Program Communications Reminders

- msroot@microsoft.com should be used for communications to ensure timely response. Emailing any other aliases may result in the email being missed.
- 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

Kernel Mode Code Signing (KMCS) Reminder

- Certs for KMCS must expire by July 1st, 2021
  - Effective for KMCS certs issued AFTER Jan 20th, 2020
  - Certificates that were able to sign drivers prior to this date may continue to sign non-driver code

- FAQ for developers found at:

  https://docs.microsoft.com/en-us/windows-hardware/drivers/install/deprecation-of-software-publisher-certificates-and-commercial-release-certificates

Note: This class of certificates goes by multiple names, such as “Driver Signing certificates”, “ Software Publisher certificates”, “Commercial Release Certificates” and “Commercial Test certificates”

Kernel Mode Code Signing (KMCS) Reminder

CommonName	ValidTo
VeriSign Class 3 Public Primary Certification Authority - G5	February 22, 2021
thawte Primary Root CA	February 22, 2021
GeoTrust Primary Certification Authority	February 22, 2021
GeoTrust Primary Certification Authority - G3	February 22, 2021
thawte Primary Root CA - G3	February 22, 2021
VeriSign Universal Root Certification Authority	February 22, 2021
TC TrustCenter Class 2 CA II	April 11, 2021
COMODO ECC Certification Authority	April 11, 2021
COMODO RSA Certification Authority	April 11, 2021
UTN-USERFirst-Object	April 11, 2021
DigiCert Assured ID Root CA	April 15, 2021
DigiCert High Assurance EV Root CA	April 15, 2021
DigiCert Global Root CA	April 15, 2021
Entrust.net Certification Authority (2048)	April 15, 2021
GlobalSign Root CA	April 15, 2021
Go Daddy Root Certificate Authority - G2	April 15, 2021
Starfield Root Certificate Authority - G2	April 15, 2021
NetLock Arany (Class Gold) Fotanúsítvány	April 15, 2021
NetLock Arany (Class Gold) Fotanúsítvány	April 15, 2021
NetLock Platina (Class Platinum) Fotanúsítvány	April 15, 2021
Security Communication RootCA1	April 15, 2021
StartCom Certification Authority	April 15, 2021
Certum Trusted Network CA	April 15, 2021

Online version of list can be found here