MICROSOFT FACE TO FACE PRESENTATION

Presenter: Hannah Sokol

PROGRAM UPDATES

OCSP Policy

CA/B Forum 61 Program Update Reminders

- Other Policies tentative for Feb 2025

All updates can be found on our blog: Program Requirements - Microsoft Trusted Root Program | Microsoft Learn

PROGRAM UPDATES

We will be updating our OCSP Policy later this month with an anticipated effective date Nov 1 such that you can use OCSP and/or CRLs

Previous:

All end-entity certificates must contain an AIA extension with a valid OCSP URL. These certificates may also contain a CDP extension that contains a valid CRL URL. All other certificate types must contain either an AIA extension with an OCSP URL or a CDP extension with a valid CRL URL

Upcoming:

All issuing CA certificates must contain either CDP extension with a valid CRL and/or an AIA extension to an OCSP responder. An end-entity certificate may contain either an AIA extension with a valid OCSP URL and/or a CDP extension pointing to a valid HTTP endpoint containing the CRL. If an AIA extension with a valid OCSP URL is NOT included, then the resulting CRL should be <10MB.

PROGRAM UPDATES

1. CRL recommendations when OCSP is not present:
    a. Should contain Microsoft-specific extension 1.3.6.1.4.1.311.21.4 (Next CRL Publish).
    b. New CRL should be available at the Next CRL Publish time.
    c. Maximum size of the CRL file (either full CRL or partitioned CRL) should not exceed 10MB.

Note: The goal of section 3.C.2- CRL Recommendations when OCSP is not present is to provide coverage for end users in cases of mass revocation.

If you have any feedback, please email msroot@microsoft.com no later than October 11, 2024.

We will be sending out an email to all once we confirm the policy and the effective date. We will also publicly post on the blog.

PROGRAM UPDATES

Initially we had announced in February 2024 at the CA/B Forum F2F 61 in New Delhi several policies to be launched in August of 2024. Due to responses internally and externally asking for more time, we have deferred these change to February 2025.

The policies were around removing EV CS OIDs, adding OIDs for EV TLS and removing S/MIME capabilities for roots without S/MIME audits.

This is a tentative date. We will send out a notification in November with testing instructions for those impacted if we move forward with the change. Please reach out to msroot@microsoft.com if you have any concerns.

CONTACT INFORMATION

Use msroot@microsoft.com to contact and for 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

THANK YOU! QUESTIONS?

TESTING EXPECTATIONS

Root Store Certificate Trust List (CTL) updated monthly (except January, July and December)

Update packages will be available for download and testing at https://aka.ms/CTLDownload - Please confirm testing when asked!

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.

Additionally, if you want to be ahead of the curve, end users can sign up to participate in the Windows Insider Build flighting program that will allow users to catch additional use cases

INCIDENT RESPONSE

Notify Microsoft promptly when facing an incident.

Negligence or non-conformance to notification requirement may result in removal.

Visit aka.ms/rootcert for guidance and email us any ongoing Bugzilla case links.

For signing certificates, monitor non-leaf certificates for private key compromise.

In case of compromise, inform us at msroot@microsoft.com for all non-revoked non-leaf certificates, including active and expired ones.

Learn more about incidents and reporting at: https://learn.microsoft.com/en-us/security/trusted-root/incident-reporting#ca-responsibilities-in-the-event-of-an-incident