MICROSOFT FACE TO FACE PRESENTATION

Presenter: Karina Goodley

AGENDA

Current Initiatives

Phase 1 Policy Updates

Contact Information

CURRENT INITIATIVES

❖ End-to-end policy refresh

  ❖ Focusing on Code Signing Requirements, TLS requirements

  ❖ Presenting phase 1 changes today. Phases 2 and 3 will be announced at upcoming F2F meetings

❖ PQC requirements to be shared at next F2F!

❖ eIDAS compliance implementation

❖ Transitioning our policy to Github with detailed changelogs coming soon!

PHASE 1 POLICY UPDATES (1 OF 2)

CP/CPS Update Deadlines: Certificate Authorities (CAs) must update their Certificate Policy (CP) and Certification Practice Statement (CPS) documents within 7 calendar days following any significant change in operations, relevant standards, or industry requirements. The updated documents must be made publicly available and communicated to Microsoft within the same timeframe. This will be effective July 1. 2025.

Revocation Response Service Level Agreement (SLA): CAs are required to respond to and process certificate revocation requests within 24 hours of receipt. This includes investigating the request, making a determination, and—if applicable—ensuring the revoked certificate's status is promptly reflected in all relevant repositories and mechanisms (e.g., CRL, OCSP). This will be effective August 1, 2025.

PHASE 1 POLICY UPDATES (2 OF 2)

Pre-Issuance Domain Validation Logging: CAs must log all domain validation events and retain these records for each TLS certificate issued. These logs must be comprehensive, timestamped, and retained for a minimum of seven (7) years. The logs should be made available to Microsoft upon request for compliance or audit purposes. This will be effective August 1, 2025.

THANK YOU! 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

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