MICROSOFT FACE TO FACE 66 PRESENTATION

Presenter: Karina Goodley

AGENDA

- Policy Updates
- Client Authentication Position
- PQC Pilot Program Plans

UPDATED POLICY WEBSITE

- You can now find us at: https://github.com/TrustedRootProgram/Program-Requirements.
- These program requirements are live, and we have redirected aka.ms/rootcert to this site. We are updating the old homepage to link to these requirements.
- We will also be putting our blog with updates in on this repo.

NEW FORMS FOR REPORTING

- **Introduced significant automation** across forms
- **Ongoing workflow optimization** to improve efficiency
- **Continuous iteration** to make forms as simple and user-friendly as possible
- **This is our starting point** for future enhancements

We will be adding these to the new site directly in the next couple of weeks.

NEW FORMS FOR REPORTING

Root Inclusion Requests

For new root inclusion requests for CAs in our program, please follow the instructions provided on the Common CA Database (CCADB) website: https://www.ccadb.org/cas/inclusion.

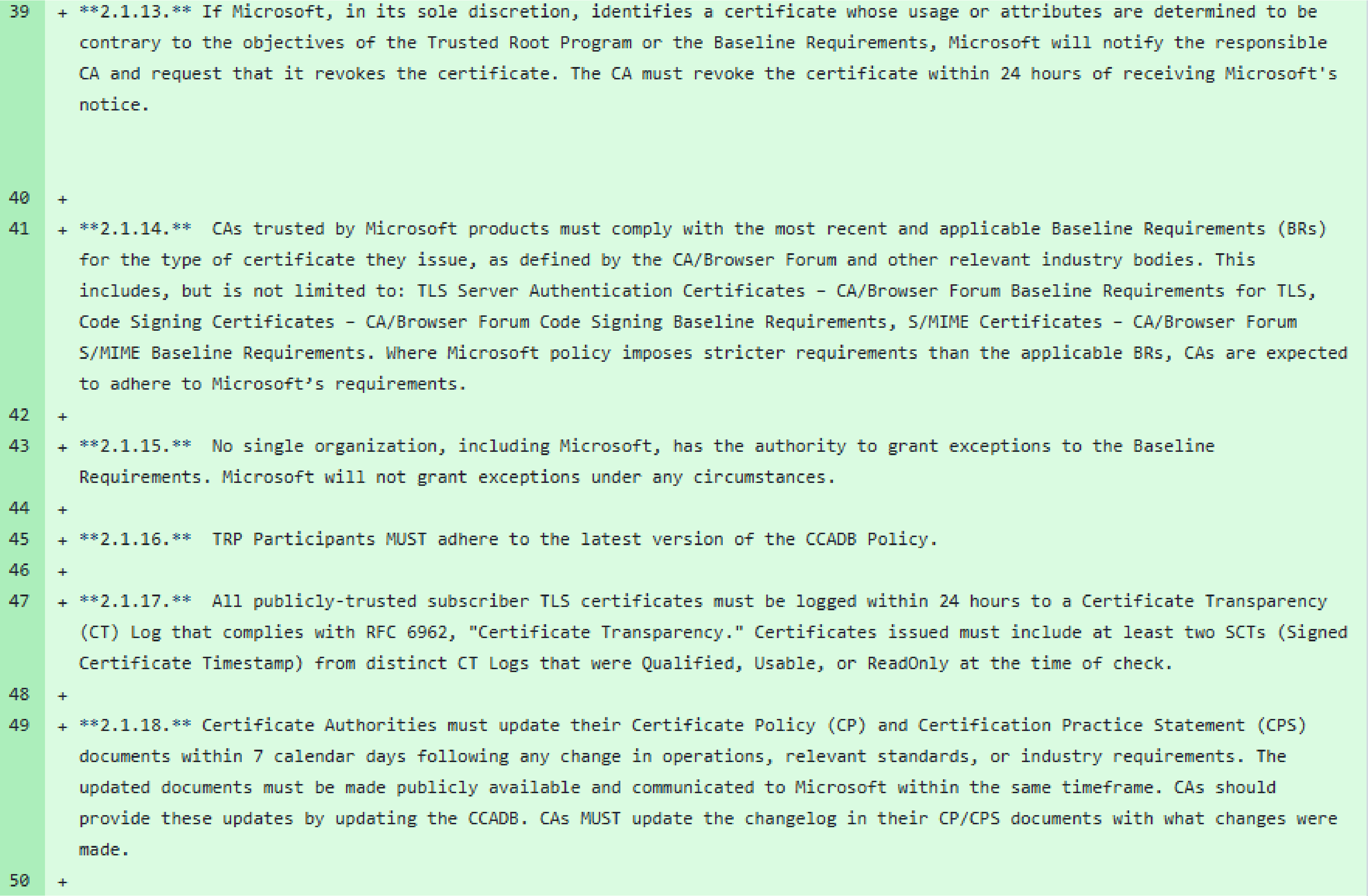
Deprecation Requests & Incident Reporting

For deprecation requests and Bugzilla/incident reports, please use the following Microsoft Forms:

Deprecation forms: https://ccadb.my.salesforce.com/sfc/p/#o0000000L7Ih/a/TO000001UFKP/Fxrco2LuUpuIYjS.ekEDbfAEg2Kwtwp1brQdDveyFA8

Bugzilla cases and incident reports: https://ccadb.my.salesforce.com/sfc/p/#o0000000L7Ih/a/TO000001UFHB/lxR9Ds5_QP0WCkRMuBv5.ZuhOLjRP6SRpy7N3onYG3U

PROGRAM UPDATES



```
+ **2.1.13.** If Microsoft, in its sole discretion, identifies a certificate whose usage or attributes are determined to be contrary to the objectives of the Trusted Root Program or the Baseline Requirements, Microsoft will notify the responsible CA and request that it revokes the certificate. The CA must revoke the certificate within 24 hours of receiving Microsoft's notice.
+
+ **2.1.14.**  CAs trusted by Microsoft products must comply with the most recent and applicable Baseline Requirements (BRs) for the type of certificate they issue, as defined by the CA/Browser Forum and other relevant industry bodies. This includes, but is not limited to: TLS Server Authentication Certificates – CA/Browser Forum Baseline Requirements for TLS, Code Signing Certificates – CA/Browser Forum Code Signing Baseline Requirements, S/MIME Certificates – CA/Browser Forum S/MIME Baseline Requirements. Where Microsoft policy imposes stricter requirements than the applicable BRs, CAs are expected to adhere to Microsoft’s requirements.
+
+ **2.1.15.**  No single organization, including Microsoft, has the authority to grant exceptions to the Baseline Requirements. Microsoft will not grant exceptions under any circumstances.
+
+ **2.1.16.**  TRP Participants MUST adhere to the latest version of the CCADB Policy.
+
+ **2.1.17.**  All publicly-trusted subscriber TLS certificates must be logged within 24 hours to a Certificate Transparency (CT) Log that complies with RFC 6962, "Certificate Transparency." Certificates issued must include at least two SCTs (Signed Certificate Timestamp) from distinct CT Logs that were Qualified, Usable, or ReadOnly at the time of check.
+
+ **2.1.18.** Certificate Authorities must update their Certificate Policy (CP) and Certification Practice Statement (CPS) documents within 7 calendar days following any change in operations, relevant standards, or industry requirements. The updated documents must be made publicly available and communicated to Microsoft within the same timeframe. CAs should provide these updates by updating the CCADB. CAs MUST update the changelog in their CP/CPS documents with what changes were made.
+
```

PROGRAM UPDATES: NEXT STEPS

- We will open comments on the PR through October 31, 2025.
- October 2025 Update by kasirota · Pull Request #5 · TrustedRootProgram/Program-Requirements
- We will consider comments and send out a final version by Nov 14, 2025 and will be effective that day.

WHAT'S NEXT?

Phase 1: Immediate Alignment with CA/B and Industry *(Current)*

Phase 2: Strengthening Technical Rigor *(2026 Q1)*

Phase 3: Audit Integrity *(2026 Q2)*

Phase 4: Operational Transparency *(2026 Q3)*

Phase 5: Ecosystem Monitoring *(2026 Q4)*

This aligns to each of the sections in our current program requirements

CLIENT AUTHENTICATION STANCE

Microsoft is committed to maintaining secure and reliable authentication for all our services. As industry standards evolve, some browsers and platforms are introducing changes to certificate trust requirements. We want to clarify our position for customers who rely on mutual TLS (mTLS) and client authentication.

Microsoft services will **continue to trust and accept certificates issued by Certificate Authorities (CAs) that include both Client Authentication and Server Authentication EKUs.**

We do **not plan to revoke existing certificates** used for mutual trust scenarios. These certificates will remain valid until their natural expiration.

We are actively working with CAs and other platforms to ensure continued availability of certificate options that meet these requirements and address operational scenarios.

PQC PILOT PROGRAM PLAN

Microsoft is launching a PQC Pilot Program for TLS Roots.

Timeline

Microsoft PKI PQC testing on in the OS will conclude soon. Once complete, TRP will send an email to all CAs in the program when we open submissions to participate in the pilot.

Supported Algorithms

- Mandatory support for **ML-DSA-87**
- Algorithm implementation must comply with published specifications.

PQC REQUIREMENTS

Certificate Specifications

Certificates must utilize only the ML-DSA-87 signature scheme for root certificates. We will not accept composite algorithms until specifications for these have been published.

Certificate profiles must adhere to X.509 standards, including proper encoding and field population.

Each certificate must include:

- Subject and issuer distinguished names, formatted per RFC 5280.
- Serial number uniqueness across the PQC root hierarchy.
- Public key information conforming to ML-DSA-87 encoding.

PQC REQUIREMENTS

Extended Key Usage (EKU) Extension

All PQC root certificates must include the EKU extension with the following OIDs: **Server Authentication** (1.3.6.1.5.5.7.3.1).

This testing will not be allowed for any non-server authentication certificates (including Code Signing, Doc Signing, Client Authentication, etc).

Validity Period Constraints

Root certificates: Maximum validity period of **1 years**.

When the root expires, it will be removed from the Root Program CTL.

Procedures for Compromised Algorithms

Immediate notification to affected CAs upon identification of algorithm compromise.

Roots will be added to the Microsoft Disallowed CTL. They will be removed when the root expires.

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