MICROSOFT FACE TO FACE 67 PRESENTATION

Presenter: Karina Goodley


SHININGPANDAS
6 7

POLICY UPDATE ROADMAP

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

Phase 2: Strengthening Technical Rigor *(Current)*

Phase 3: Audit Integrity *(2026 H2)*

Phase 4: Operational Transparency *(2027 H1)*

Phase 5: Ecosystem Monitoring *(2027 H2)*

MICROSOFT POLICY UPDATE GOALS FOR PHASE 2

- Reduce blast radius and long-term cryptographic risk
- Improve auditability, incident response, and ecosystem transparency
- Align trust anchors with modern lifecycle and automation expectations
- Improve consistency across Microsoft security programs and industry norms

SUMMARY OF PROPOSED PHASE 2 POLICY CHANGES

Area	Change Type	Effective Date
Root certificate lifetime	Modification	July 1, 2026
Root EKU separation	New requirement	July 1, 2026
Bugzilla incident disclosure	New requirement	April 1, 2026
Suspect code definitions	New clarification	April 1, 2026

SHORTER LIFESPANS FOR ROOT CERTIFICATES

- Newly minted Root CA certificates are limited to **a maximum validity of 10 years**
- The lifetime limit applies to **both the certificate and the underlying key material**
- **Root key reuse is not permitted**
- After expiration, a **new root and new key material** must be generated and submitted

> **3.1.8.** Newly minted Root CAs must be valid for a ~~minimum of eight years, and a maximum of 25 years, from the date of submission~~maximum 10 years, from the date of submission, effective July 1, 2026.

SEPARATION OF TRUST PURPOSES AT THE ROOT LEVEL

- Root certificates must be dedicated to a clearly defined trust purpose
- Server Authentication, S/MIME, and Code Signing must each use separate roots
- These EKUs must not be combined with one another
- Other EKUs (Client Auth, Time Stamping) can be combined or separate
- **Yes, this does still allow for Server Auth and Client Auth to be together on the same root**

```
+ **3.4.3** Effective for all root certificates submitted on or after July 1, 2026:
+ Effective for all root certificates submitted on or after July 1, 2026, root certificates MUST be limited
  in scope and dedicated to a clearly defined trust purpose.
+ Root certificates authorized for Server Authentication, S/MIME, or Code Signing MUST each be separate and
  independent trust anchors. A root certificate MUST NOT be authorized for more than one of these EKUs.
+ A root certificate authorized for Code Signing MAY also be authorized for Client Authentication and Time
  Stamping. A root certificate authorized for Server Authentication OR SMIME MAY also be authorized for
  Client Authentication.
+ No EKU combinations other than those explicitly permitted above are allowed.Root certificates submitted
  prior to January 1, 2027 that assert multiple EKUs will continue to be trusted unless otherwise directed
  by Microsoft.
```

INCIDENT DISCLOSURE AND TRANSPARENCY

- Certificate Authorities must **publicly disclose and/or respond to incidents in Bugzilla**
- Applies to **all incidents,** including low-impact or procedural issues
- Incidents must follow **CCADB Incident Report format and timelines**
- If not yet disclosed, CAs must notify **msroot@microsoft.com** promptly

```
+ **2.1.18** Certificate Authorities MUST publicly disclose and/or respond to
  incident reports in Bugzilla, including incidents that the Program Participant
  believes to be low-impact, procedural, or non-security-relevant. Incident reports
  MUST be submitted in accordance with the current CCADB Incident Report format and
  applicable disclosure timelines, which can be found here:
  <https://www.ccadb.org/cas/incident-report>. If a Program Participant has not yet
  publicly disclosed an incident in Bugzilla, the Participant MUST promptly notify
  msroot [at] microsoft.com and MUST provide an initial public disclosure timeline.
+
```

SUSPECT CODE CLASSIFICATION

Microsoft uses **consistent criteria across security products**

Definitions align with Microsoft's **Unified Security Operations criteria**

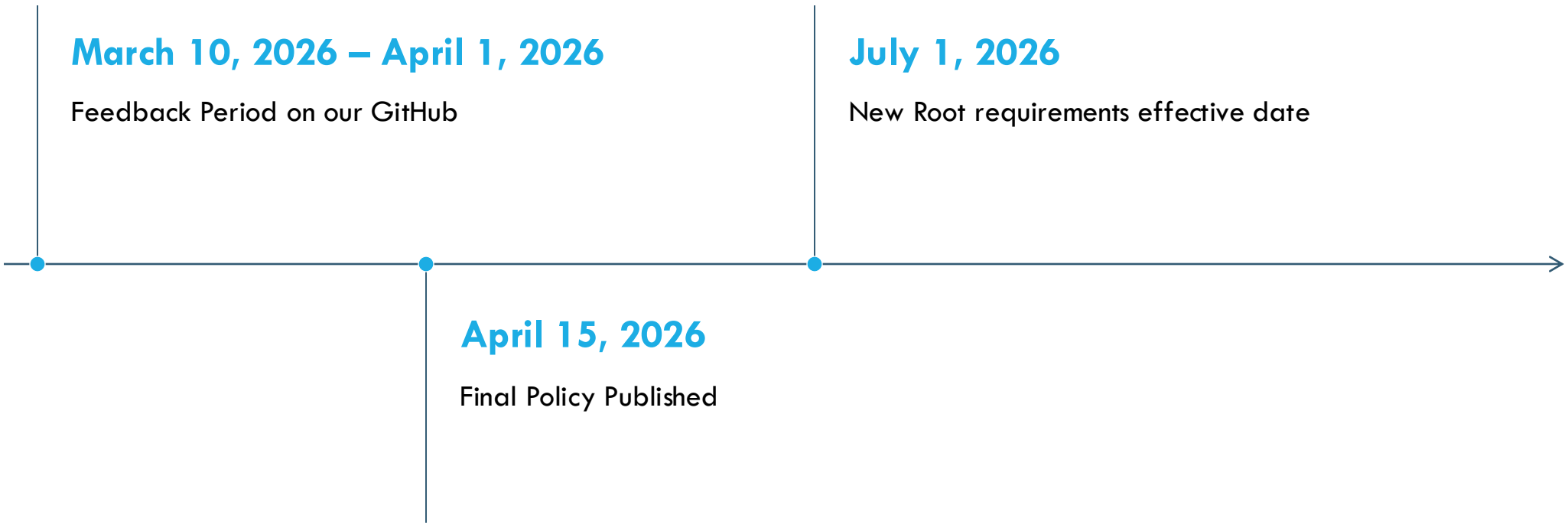
Helps CAs understand how code behavior may be assessed during:

- Incident investigation
- Disclosure
- Enforcement actions

Link:
https://learn.microsoft.com/en-us/unified-secops/criteria

> **3.3.3** For clarity and transparency, Microsoft and the Microsoft Trusted Root Program classify "suspect code" using the same criteria applied across Microsoft security products. These classifications are documented in Microsoft's Unified Security Operations criteria, which describe how Microsoft identifies and categorizes malware, potentially unwanted applications, tampering software, and related behaviors: <https://learn.microsoft.com/en-us/unified-secops/criteria>. These definitions are provided to assist Program Participants in understanding how Microsoft may assess code behavior during incident investigation, disclosure, and enforcement activities.

PHASE 2 TIMELINE



PHASE 2 NEXT STEPS

- We will open comments on the PR through April 1, 2026.
- March 2026 update by kasirota · Pull Request #20 · TrustedRootProgram/Program-Requirements (or https://aka.ms/march2026update as a short link)
- We will consider comments and send out a final version via email by April 15, 2026 and will be effective that day.

LOOK AHEAD TO PHASE 3 UPDATES

Area	Change Type
Trust Anchor Identifiers	New (proposed)
ACME for TLS	Future addition
Microsoft CT log list	Future addition

TRUST ANCHOR IDENTIFIERS

In the future (at some point), TLS Roots must be associated with a **Trust Anchor Identifier**

Aligned with the IETF **TLS Trust Anchor Identifiers** draft

Identifier:

- Uniquely identifies a single trust anchor
- Remains stable for its lifetime
- Is **not required to be embedded in the certificate**

Used consistently in:

- CCADB
- Incident reports
- Program communications

Link (clickable):
https://www.ietf.org/archive/id/draft-ietf-tls-trust-anchor-ids-02.html

FUTURE ADDITIONS

Mandate **ACME protocol support** for automated TLS issuance

Maintain a **Microsoft-approved list of CT logs**

Details to be announced in **September TRP update**

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

UPDATED POLICY WEBSITE

- You can now find us at: https://github.com/TrustedRootProgram/Program-Requirements (or aka.ms/rootcert as a short link)
- We will also be putting our blog with updates in on this repo.

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