Microsoft CA/B Forum F2F 61

Presenters: Nitesh Bakliwal

On Behalf of Microsoft TRP Group

Agenda

- Program Updates
  - CTL Monitor Policy Debut
  - Remove EV CS OID
  - EV TLS CA/B Forum OID
  - S/MIME Audit Requirement
  - Windows incompatibility with ECC Code Signing
  - OCSP Policy
- TRP CA Survey
- Refresher (Call to Action)
  - Testing Expectations
  - Incident Response
- How to reach us?

Program Updates and New Policies

Certificate Transparency Policy
(for TLS Certs)

Allows Microsoft Web Applications to have consistent trust with browsers or need to meet regulatory requirements the ability to do so through CT

Formal verbiage will be posted on our Security Blog: https://learn.microsoft.com/en-us/security/trusted-root/program-requirements

On February 2024, Microsoft will be appending Certificate Transparency policy to Crypt32 in Windows which will check for the presence of Signed Certificate Timestamp (SCT) for the TLS certificate to be valid

The policy will be in audit mode for Windows for now with the goal being that other applications will start enforcing the policy by end of 2024. Initially, Microsoft will leverage approved log list from Apple and Google as baseline.

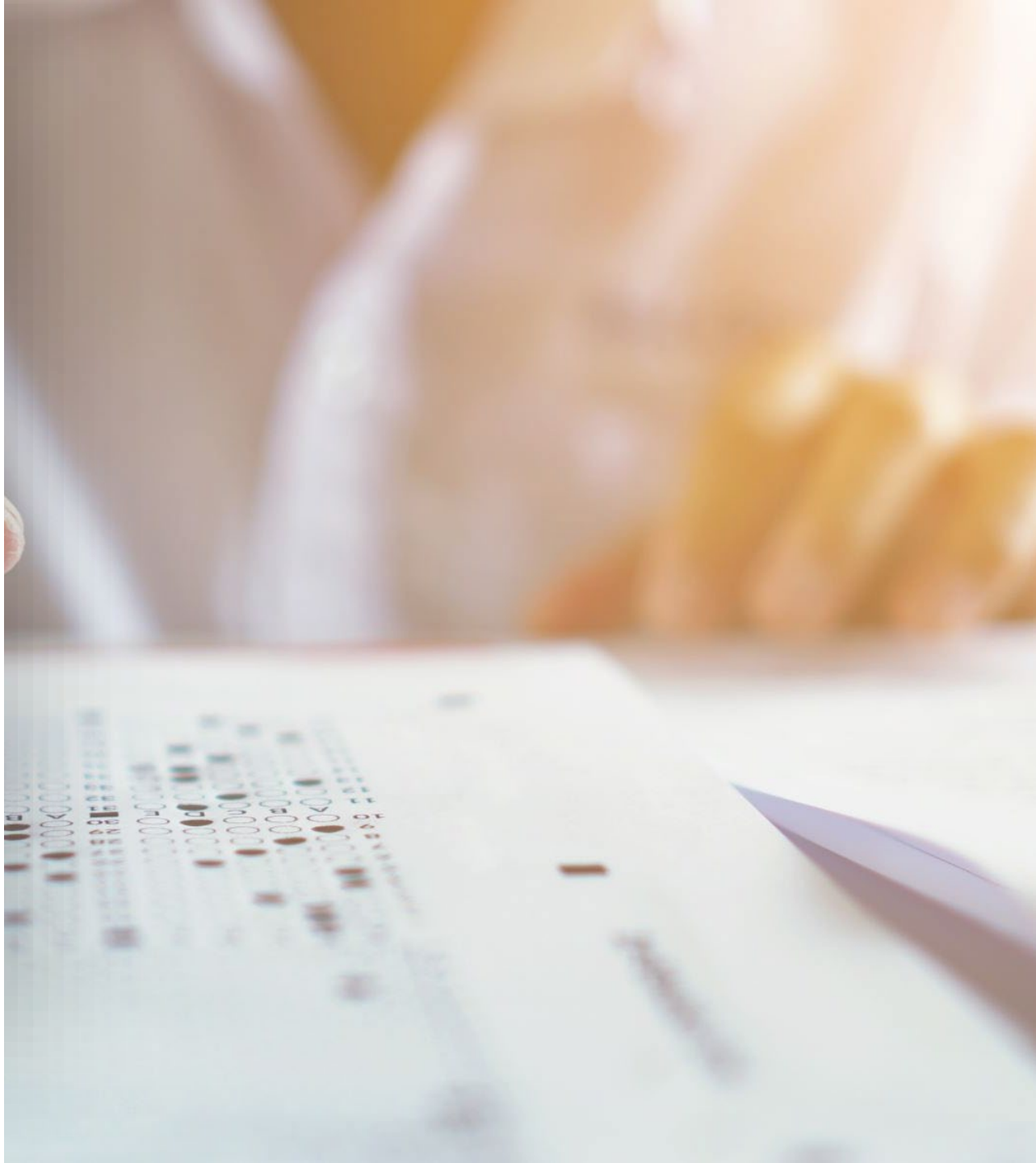
Note: CAs were given the heads up and deadline of **December 1st, 2023,** to raise any issue or stress point around it, that need further support.

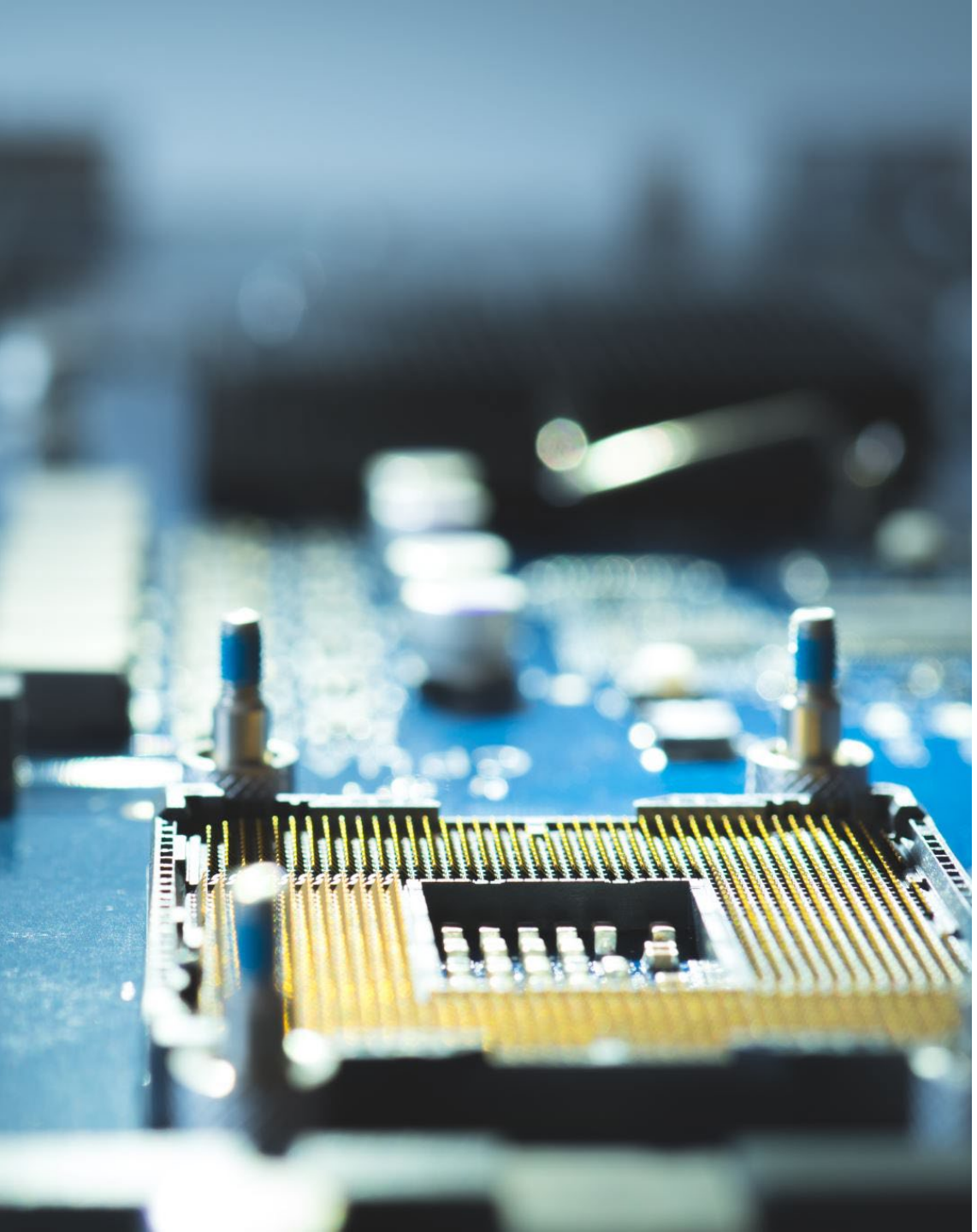
CT Log Monitors MS will Reference

Google 'Argon2023' log	Let's Encrypt 'Oak2025h1'	Cloudflare 'Nimbus2023' Log
Google 'Argon2024' log	DigiCert Nessie2024 Log	Cloudflare 'Nimbus2024' Log
Google 'Argon2025h1' log	DigiCert Nessie2025 Log	Cloudflare 'Nimbus2025' Log
Google 'Argon2025h2' log	Sectigo 'Sabre' CT log	Let's Encrypt 'Oak2025h2'
Google 'Xenon2023' log	Sectigo 'Sabre2024h1	Trust Asia Log2023
Google 'Xenon2024' log	Sectigo 'Sabre2024h2'	Trust Asia Log2024-2
Google 'Xenon2025h1' log	Sectigo 'Sabre2025h1'	TrustAsia Log2025a
Google 'Xenon2025h2' log	Sectigo 'Sabre2025h2'	TrustAsia Log2025b
Let's Encrypt 'Oak2023' log	Sectigo 'Mammoth' CT log	DigiCert Yeti2024 Log
Let's Encrypt 'Oak2024H1' log	Sectigo 'Mammoth2024h2'	DigiCert Yeti2025 Log
Let's Encrypt 'Oak2024H2' log		DigiCert Nessie2023 Log

Removing EV Code Signing OID

- Removing EV CS Audit Requirement from program
- Removing EV CS OIDs from roots in August 2024 release
- Let us know if there are issues by April 1st 2024 via our email msroot@microsoft.com





Updating Certificates with CA/B Forum EV SSL OID

- Requiring that all EV SSL Certificates have the CA/B Forum Standard EV SSL OID (2.23.140.1.1)
- Making change in the August 2024 TRP CTL Release
- We will be reaching out to CAs that are affected by this change to talk through next steps.
- In the meantime, if these changes cause concern please reach out by April 1st 2024 via our email msroot@microsoft.com

S/MIME Audit Requirement

- Adding S/MIME Audit requirements for all roots with Secure Email Trust Bits
- If CA is not compliant by June 2024, Microsoft will make an action to remove trust bit in August 2024 release
- Audits Excepted by:
  - WebTrust Principles and Criteria for Certification Authorities – S/MIME
  - ETSI EN 119 411-6 LCP, NCP, or NCP+
- Let us know by April 1st if you foresee this deadline being an issue for your company via our email msroot@microsoft.com

Windows incompatibility with ECC Code Signing

- While in general, Windows does not reject code signed with an ECC certificate, there are key applications/features that do not accept it.
- We have updated our policy to say that these certs will run into incompatibility issues with these programs
- There are currently no plans to make this algorithm compatible, given the development of compatibility with PQC certs algorithms

OCSP Policy

- There are no changes to the Microsoft OCSP requirement- it is still required.
- There is currently no timeline for when we will be able to change this requirement.
- This will continue to be a requirement through June 2024 at a minimum and will be revisited then.

Survey, Testing, and Incident Response

Trusted Root Program CA Survey

We want to hear from you!

On Tuesday, February 20th all CAs should have received an email from msroot@microsoft.com requesting participation in the Microsoft TRP Survey.

Response requested by March 15th, 2024

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 a tmsroot@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

How to reach us?

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