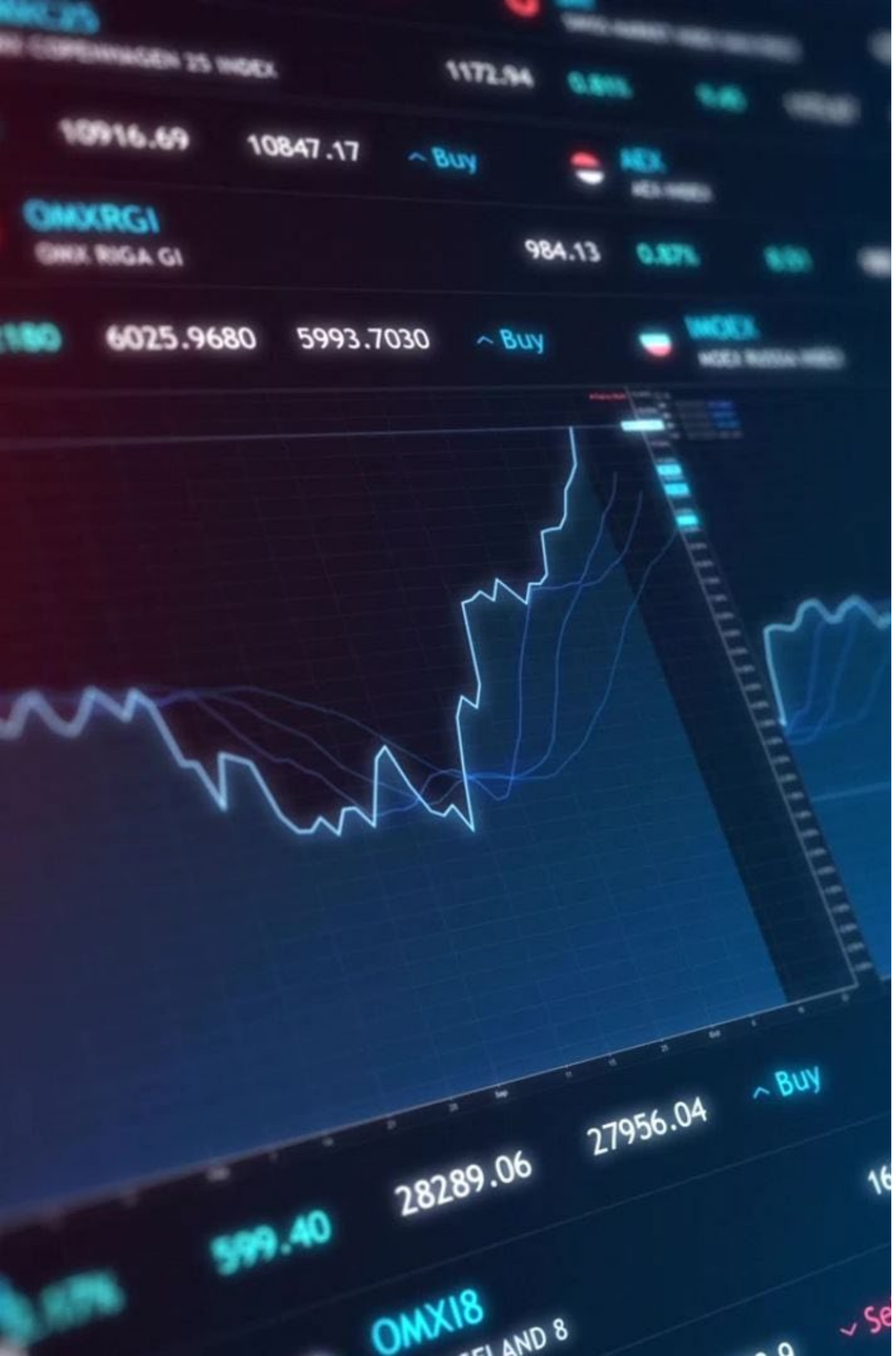
Microsoft CA/B Forum F2F 60

Presenters:

Hannah Sokol
Nitesh Bakliwal

Agenda

- Program Updates
  - CTL Monitor Policy
- Best Practices Reminder
- Refresher (Call to Action)
  - Testing Expectations
  - Incident Response
- How to reach us?



Program Updates

- Microsoft will continue to support only RSA for Code Signing Certificates
- Microsoft would not be making OCSP optional at this time due to platform constraints.
- As of February 1st, 2024, Microsoft will start auditing that all TLS certificates have a Signed Certificate Timestamp (SCT) with the intention to start enforcing it in the future

Certificate Transparency Policy

✓ Allows Microsoft Web Applications that wish 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 certificate to be valid

The policy will be in audit mode for Windows for now, however, other applications will start enforcing the policy mid 2024

Please let the TRP team know **by December 1st, 2023** if you foresee this being an issue or stress point for your organization at msroot@microsoft.com

Best Practices Reminder

We have seen that end-entity customers experienced multiple outages due to inconsistent Cert management practices. It also results in potential security risks for them and the ecosystem. During our engagements, we noticed that many of these customers aren't even aware of the best practices around Cert management.

Call to Action to all CAs: Please double down in informing and educating end-entity customers of Cert management best practices, to help reduce security risks and business device outages.

References: Here are two great resources for Best Practices for Certificate Management. Please pass this information along to your customers to ensure they continue to operate to the best of their ability

Technical Best Practices

- https://www.ccadb.org/documents/TSP_Technical_Best_Practices_eIDAS.pdf

Time Stamping Instructions

- https://learn.microsoft.com/en-us/windows/win32/seccrypto/time-stamping-authenticode-signatures

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.
- Use the incident reporting form at aka.ms/rootcert or email an ongoing Bugzilla case link.
- 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

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