Microsoft

Microsoft Trusted Root Program Update

CA/Browser Forum
Face to Face Meeting 47 Thessaloniki
June 12, 2019

Agenda

- Intro of Microsoft Attendees
- Program Communications
- Microsoft Root Change Terminology
- Program Updates
- Microsoft Edge and Chromium Open Source

Program Communications Reminders

- msroot@microsoft.com should be used for communications to ensure timely response
- Program requirements can be found on Microsoft Docs (https://docs.microsoft.com/en-us/) at: https://aka.ms/RootCert
- Program audit requirements can be found on Microsoft Docs at: https://aka.ms/auditreqs

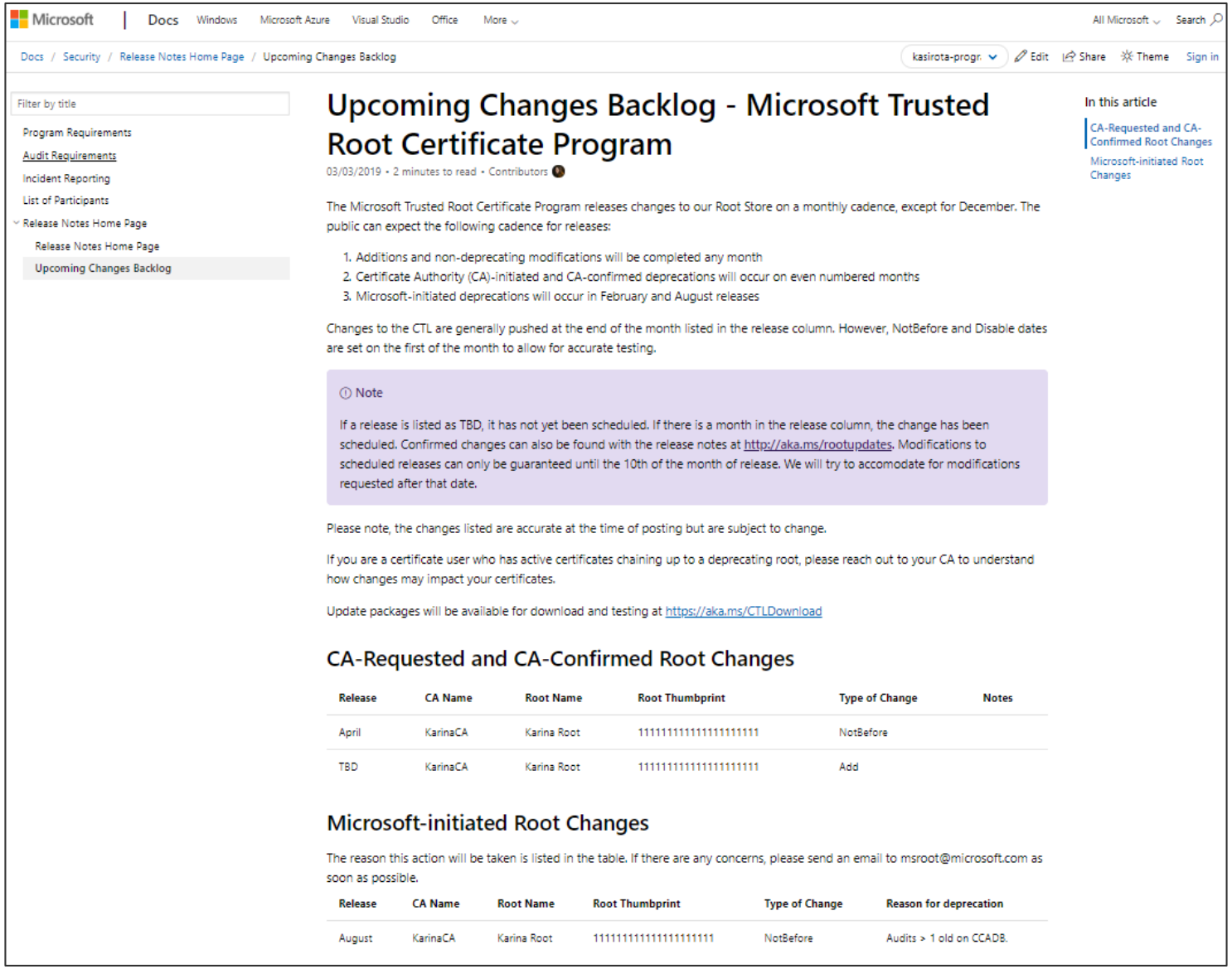
Microsoft Root Change Terminology

Disallow	Designed for major security incidents. Certificates added to the Disallowed list can be issuing or leaf certificates and DO NOT need to be in the Certificate Trust List (CTL). Disallowed certificates are blocked from being trusted
Removal	Removal of root from the Certificate Trust List. All certificates no longer trusted
Disable	Introduced in Windows10RS1. Disables all certificates issued by the root certificate except for Code Signing and Time Stamping. Code Signing and Time Stamping certificates will continue to be trusted if the certificate was issued prior to the Disable date
NotBefore	Introduced in Windows10RS2. Allows granular disabling of a root certificate or specified EKU capabilities of a root certificate. The NotBefore property distrusts the certificate or specified EKU if it was issued after the NotBefore date. Certificates issued prior to the NotBefore date will not be impacted

Program Updates

- Root Store Certificate Trust List (CTL) updated monthly (except December)
  - Additions and non-deprecating modifications will be completed any month
  - CA-initiated and CA-confirmed deprecations will occur on even numbered months (e.g. Feb, Apr, Jun, Aug, Oct)
  - Microsoft-initiated deprecations will occur in February and August releases
  - Release notes at https://docs.microsoft.com/en-us/security/trusted-root/release-notes
- Plan to publicly share backlog of pending root store changes starting by July (preview in next slide)
- Initiated vetting of all new CA applicants and will review existing CAs at least annually. Includes:
  - Beneficial Ownership Screening
  - Anti-Corruption
  - Business Verification
  - Trade Sanctions
  - Other due diligence as appropriate

Upcoming Changes Backlog Preview



Microsoft | Docs Windows Microsoft Azure Visual Studio Office More All Microsoft Search

Docs / Security / Release Notes Home Page / Upcoming Changes Backlog kasirota-progr Edit Share Theme Sign in

Filter by title

- Program Requirements
- Audit Requirements
- Incident Reporting
- List of Participants
- Release Notes Home Page
  - Release Notes Home Page
  - Upcoming Changes Backlog

Upcoming Changes Backlog - Microsoft Trusted Root Certificate Program

03/03/2019 • 2 minutes to read • Contributors

In this article

- CA-Requested and CA-Confirmed Root Changes
- Microsoft-initiated Root Changes

The Microsoft Trusted Root Certificate Program releases changes to our Root Store on a monthly cadence, except for December. The public can expect the following cadence for releases:

1. Additions and non-deprecating modifications will be completed any month
2. Certificate Authority (CA)-initiated and CA-confirmed deprecations will occur on even numbered months
3. Microsoft-initiated deprecations will occur in February and August releases

Changes to the CTL are generally pushed at the end of the month listed in the release column. However, NotBefore and Disable dates are set on the first of the month to allow for accurate testing.

ⓘ Note

If a release is listed as TBD, it has not yet been scheduled. If there is a month in the release column, the change has been scheduled. Confirmed changes can also be found with the release notes at http://aka.ms/rootupdates. Modifications to scheduled releases can only be guaranteed until the 10th of the month of release. We will try to accomodate for modifications requested after that date.

Please note, the changes listed are accurate at the time of posting but are subject to change.

If you are a certificate user who has active certificates chaining up to a deprecating root, please reach out to your CA to understand how changes may impact your certificates.

Update packages will be available for download and testing at https://aka.ms/CTLDownload

CA-Requested and CA-Confirmed Root Changes

Release	CA Name	Root Name	Root Thumbprint	Type of Change	Notes
April	KarinaCA	Karina Root	11111111111111111111	NotBefore	
TBD	KarinaCA	Karina Root	11111111111111111111	Add	

Microsoft-initiated Root Changes

The reason this action will be taken is listed in the table. If there are any concerns, please send an email to msroot@microsoft.com as soon as possible.

Release	CA Name	Root Name	Root Thumbprint	Type of Change	Reason for deprecation
August	KarinaCA	Karina Root	11111111111111111111	NotBefore	Audits > 1 old on CCADB.

- Allows certificate users who have active certificates chaining up to a deprecating root to be made aware of changes that may impact their certificates
- Update packages will be available for download and testing at https://aka.ms/CTLDownload

Microsoft Edge and Chromium Open Source

- We will adopt Chromium as the web platform for Microsoft Edge
- We intend to become a significant contributor to Chromium
- Microsoft Edge will be delivered and updated for all supported versions of Windows and on a more frequent cadence
- Preview builds are available for insight into our testing and contributions. Feedback is encouraged. Go to: https://www.microsoftedgeinsider.com/