Microsoft

Microsoft Trusted Root Program Update

CA/Browser Forum
Shanghai China Face to Face Meeting
October 17, 2018

Agenda

- Program Reminders
- Microsoft Root Change Terminology
- Program Updates
- Plan for Updating Program Audit Requirements
- Symantec Roots
- Certificate Transparency

Program Reminders

- msroot@microsoft.com should be used for communications to ensure timely response
- Program requirements can be found at: http://aka.ms/RootCert
- Program audit requirements can be found at: http://aka.ms/auditreqs

Microsoft Root Change Terminology

Removal	Removal of root from the Certificate Trust List (CTL). 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 CA application updated (http://aka.ms/rootcertapply)
- New forms required for CA initiated requests to modify existing roots or add new roots. Contact msroot@Microsoft.com
- Root Store Certificate Trust List (CTL) updated monthly (except December). Changes posted at http://aka.ms/rootupdates
- We are exploring the possibility of publicly sharing pending root store changes (our backlog). More information to follow at March 2019 CA/Browser Forum meeting

Program Updates - Continued

- Continued end-to-end examination of each root in the root store for EKUs, use, contract compliance and other issues which may represent risk to Microsoft customers
- Continued efforts toward automation of program processes to minimize errors and enable increased verification of program compliance
- We now send automated emails to all CAs that have changes in a release requesting that they test

Plan for Updating Program Audit Requirements

- Updating audit requirements to the newest versions as of January 1, 2019
  - New versions on aka.ms/auditreqs will be available by October 31, 2018
  - Latest standards must apply to audits commencing on or after January 1, 2018
- *WebTrust Trust Services Principles and Criteria for CAs – Code Signing* will be required for CAs with code signing EKU
  - If a CA has the code signing EKU enabled on a root but is not actively issuing code signing certificates, we will change their EKU status set to "NotBefore."
  - If a CA is issuing EV code signing certificates, they will still be required to provide the WebTrust Principles and Criteria for CAs – EV Code Signing audit, in addition to the Code Signing audit
- CAs using the ETSI audit scheme must provide audits in EN 319 411-1 or EN 319 411-2 audit schemes

Symantec Roots

- Microsoft and DigiCert partnered to create a deprecation schedule for TLS certificates that took into account the needs of our mutual customers and compliance
- Plan published on our “Microsoft Secure” blog (LINK)
- DigiCert is developing plans to deprecate other capabilities

Certificate Transparency

- Microsoft currently evaluating a CT enforcement policy
- Participating in CT Policy Days (November 6-7, 2018)
- CT Log planned for 2019
- Below are two posts from Microsoft on CT, both focused on our Active Directory Certificate Services (ADCS) users
  - https://blogs.technet.microsoft.com/pki/2018/03/12/how-will-certificate-transparency-affect-existing-active-directory-certificate-services-environments/
  - https://support.microsoft.com/en-us/help/4093260/introduction-of-ad-cs-certificate-transparency