Microsoft Root Certificate Program

This document lists the details and requirements for the Microsoft Root Certificate program.

Program Requirements

In order to better protect Microsoft customers from security issues related to the use of PKI certificates, and to generally enhance the end-user experience for Windows users, Microsoft is moving to standardize and tighten the criteria for Root Certificate Authorities in Windows XP and future operating system releases. This standard also applies to Root Certificate Authorities in Internet Explorer and any other Microsoft product. Some highlights of the new standards:

- CA providers will be required to complete a WebTrust for Certification Authorities audit or provide an equivalent third-party attestation. For more information on the AICPA's WebTrust for Certification Authorities Program, or to obtain a copy of the criteria, see http://www.webtrust.org/certauth.htm. If you have received an audit other than Webtrust for CA's, the burden is on the CA to prove equivalency to WebTrust for CA's.
- Only roots that expire after Jan 1, 2010 will be included.
- Up to three roots per CA provider can be accepted, since each additional root negatively impacts user by increasing download time.
- Microsoft will require each certificate issued from each CA provider's root(s) for testing purposes. We recommend that you send us a URL of a publicly accessible server where certificates issued from your roots can be verified.
- All new Root Certificate Authorities for Whistler and future operating system releases will be made seamlessly available to end users through the Windows Update Certificate Trust List ("CTL"). This provides maximum flexibility for both CA providers and for Microsoft to respond immediately in the event of an unforeseen security issue.
- Your root certificate must provide broad business value to Microsoft platform customers. For example, root certificates used internal to an organization are not acceptable for the root program.
- Certificates issued from your root should support the CDP extension. The CDP should point to a location that is publicly accessible.

Change in Root Delivery Process

New root certificates no longer ship with Microsoft Internet Explorer. They ship through the platform. Any new roots accepted by Microsoft will be made available to Windows XP clients as part of a seamless root update mechanism using Windows Update. When a user visits a secure web site (using HTTPS), reads a secure email (S/MIME), or downloads an ActiveX control that uses a new root certificate, the Windows XP certificate chain verification software will check this Windows Update location and download the needed root certificate. To the user, the experience is seamless. The user sees no security dialogs or warnings. The download happens automatically and behind the scenes.

New roots will also be made available to down-level clients through a Windows Update download item first available in 2001. This item will update Windows 2000, Windows NT, Windows 95, Windows 98, and Windows Millennium Edition (ME) clients.

Root Acceptance Schedule

Once you have met all of the requirements and Microsoft has accepted your root certificate, it will be made available on the web to Windows XP and down-level platform users at the next refresh interval. The list of root certificate authorities on Windows Update will be updated at least once a quarter.

DO NOT SEND ANY ROOT CERTIFICATES UNTIL YOU HAVE BEEN ACCEPTED BY MICROSOFT.

You must complete all requirements of the program before we will process your root certificate.

First Steps

To begin the root acceptance process, perform the following steps:
Send an e-mail with the following information to casubmit@microsoft.com

1. Two contacts from your organization (name, e-mail, and phone)
2. Company name and address information
3. Company web page
4. Number of roots you would like to submit
5. Please answer the following questions about your root certificates:
    a. What are the root certificates used for (e.g. e-mail, SSL, code-signing, etc)
    b. To whom will you issue certificates? (i.e. the general public, members of a certain organization?)
6. Pointers to Certificate Practice Statement
7. List of any third-party audits your CA practice has undergone.

You should ensure the services your root will be used for provide broad value to Microsoft customers. If you have questions concerning this, you should send e-mail to casubmit@microsoft.com. Next, you should engage a licensed auditor of the WebTrust for CA's program and complete that process.

Submission of Root

Once you have met all the criteria for acceptance by our program, send the following to the address below:

1. Audit report
2. A letter on corporate letterhead, by an authorized agent of the company detailing the following for each root that is submitted.
    a. Root certificate Subject name, validity dates, and SHA-1 thumbprint. You can view the thumbprint by double-clicking the root certificate in explorer, selecting the Details tab, and scrolling down to the thumbprint field.
    b. Desired Extended Key Usage. For what usages should this root be marked: SSL server auth, e-mail, code signing, etc.
    c. Please send an HTTPS URL or certificate issued from the root that can be used for chain validation testing.

Please send all paperwork to:

Microsoft Root Certificate Program
c/o John Lambert (johnla@microsoft.com)
Program Manager, Windows Security
Bldg 40/6195
Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052

Frequently Asked Questions

1. How much does the program cost?
   Microsoft does not currently charge for the program. Normally there is a material cost associated with meeting the audit requirements. Please contact your auditor or visit the following web page for more details: http://www.webtrust.org/certauth.htm, section titled "How much does a Web Trust for CA examination cost?"

2. Is [insert audit here] sufficient for WebTrust equivalency?
   The burden is on the CA to prove WebTrust equivalency. Your auditor should state in their audit report whether the audit meets the WebTrust criteria.

3. What is the deadline for submitting my root certificate?
   Microsoft is accepting roots on an on-going basis. As such, there is no hard deadline. Once your root certificate is accepted, it will appear on Windows Update after the next root certificate refresh cycle.