Microsoft Trusted Root Certificate: Program Requirements

1. Introduction

The Microsoft Root Certificate Program supports the distribution of root certificates, enabling customers to trust Windows products. This page describes the Program's general and technical requirements, including information about how a Certificate Authority (CA) can contact Microsoft to request inclusion into the program.

2. Certificate Authority Intake Process

1. In order to begin the process to be included in the Program, a CA must fill out the application located at http://aka.ms/rootcertapply and email the completed form to trustcert@microsoft.com. This will begin the onboarding process, outlined below:

2. Microsoft will review the application, and may request additional documentation from the CA to determine if the CA meets the Program requirements and whether, in Microsoft's judgment, the CA's inclusion into the program will benefit Microsoft's customers.

3. Microsoft will provide preliminary Program approval to the CA and a deadline by which all materials must be completed and returned to Microsoft, for the CA to in included in the next release (typically every four months).

4. Upon receipt of preliminary approval from Microsoft, the CA will need to engage an auditor to complete the necessary audit. See, http://aka.ms/auditreqs for more information about the Program's audit requirements.

5. When the audit is complete, the CA must send the following materials to Microsoft:
    a) A copy of all of the roots that the CA wishes to have Microsoft include in the Program in .cer file format (contained in a .ZIP file)
    b) Test URLs for each root, or a URL of a publicly accessible server that Microsoft can use to verify the certificates.
    c) An electronic copy or URL that contains the most recent audit attestation for each of the roots the CA wishes to have Microsoft include in the Program
    d) Information to complete and sign the Program contract, including:
        i. The name, email address, phone number, and job title of the person who will sign the Program contract
        ii. A second contact's name, email address, and phone number.
        iii. The company's principle place of business (street address).
        iv. The company's place of incorporation (country or state/province).
6. Microsoft will send the Program contract to the CA to sign and return to Microsoft.

7. Upon receipt of the completed contract, Microsoft will add the CA to the next release, if the CA has returned the materials by the deadline provided to the CA. Otherwise, Microsoft will add the CA's roots to a subsequent release.

Note
Microsoft will determine at its sole discretion which CA certificates are included the Program. Microsoft will not charge any fee for including a CA's certificates in the Program. Microsoft reserves the right to not include a CA in the Program for any reason or no reason at all

3. Continuing Program Requirements

1. The CA must provide to Microsoft evidence of a Qualified Audit (see http://aka.ms/auditreqs) for each root, non-limited sub-~~root~~CA, or cross-signed non-enrolled root, before conducting commercial operations and thereafter on an annual basis.

2. The CA must assume responsibility to ensure that all non-limited sub-~~roots~~ CAs and cross-signed, non-enrolled roots meet the Program Audit Requirements.

3. The CA must provide Microsoft with updated Program contacts every July, November, and March, as well as upon Microsoft's request.

4. The CA must disclose its full PKI hierarchy (non-limited sub-~~roots~~CAs, cross-signed non-enrolled roots, intermediates, EKUs, certificate restrictions) to Microsoft on an annual basis, including certificates issued to CAs operated by external third parties. More about the depth of sub-CA (define as all below root)

5. CAs must inform Microsoft at least 120 days before transferring ownership of an enrolled root to another entity or person, and obtain Microsoft's consent prior to transfer.

6. CAs must designate and disclose to Microsoft at least two contacts to be responsible to receive communications from Microsoft, including contact names, email addresses, and business and mobile phone numbers.

7. CAs must agree to receive notices by e-mail and must provide Microsoft with an email address to receive official notices. If Microsoft sends an email that is undeliverable, Microsoft will send notices to the last-known address for the CA. CAs must agree that notice is effective when Microsoft sends the email or the letter.

8. CAs must agree that Microsoft may contact customers that Microsoft believes may be substantially impacted by Microsoft's decision to remove a root from the Program.

9. CAs may not enroll a root into the Program that is intended to be used internally within an organization (i.e. Enterprise CAs).

10. CAs must publicly disclose all audit reports for non-limited sub-roots.

11. If a CA uses a subcontractor to operate any aspect of its business, the CA must assume responsibility for the subcontractor's business operations.

4. Program Technical Requirements

All CAs in the Program must comply with the Program Technical Requirements. If Microsoft determines that a CA is not in compliance with the below requirements, Microsoft will exclude that CA from the Program.

A. Root Requirements

1. Root certificates must be x.509 v3 certificates.

    a) The CN attribute must identify the publisher and must be unique.

    b) The CN attribute must be in a language that is appropriate for the CA's market and readable by a typical customer in that market.

    c) Basic Constraints extension: must be cA=true.

    d) Key Usage (if present) must be keyCertSign and cRLSign only.

        i. Root Key Sizes must meet the requirements detailed in "Key Requirements".

2. New roots must be valid for at least eight (8) years from the date of submission.

3. New ~~R~~root certificates must expire no more than 25 years after the date of application for distribution.

4. The CA may not issue new 1024-bit RSA certificates for SSL/TLS or Code Signing from roots covered by these requirements.

5. All end-entity server authentication certificates must contain an AIA extension with a valid OCSP URL. These certificates may also contain a CDP extension that contains a valid CRL URL. All other certificate types must contain either an AIA extension with an OCSP URL or a CDP extension with a valid CRL URL

6. Private Keys and subject names must be unique per root certificate; reuse of private keys or subject names in subsequent root certificates by the same CA may result in random certificate chaining issues. CAs must generate a new key and apply a new subject name when generating a new root certificate prior to distribution by Microsoft.

7. All roots that are being used to issue new certificates, and which directly or transitively chain to a certificate included in the Program, must either be limited or be publicly disclosed and audited.

8. Government CAs must restrict server authentication to .gov domains and may only issues other certificates to the ISO3166 country codes that the country has sovereign control over (see http://aka.ms/auditreqs section III for the definition of a "Government CA").

9. Government CAs that also operate as commercial, non-profit, or other publicly-issuing entities must use a different root for all such certificate issuances (see http://aka.ms/auditreqs section III for the definition of a "Commercial CA").

10. New ~~I~~intermediate CA certificates must meet the requirements for algorithm type and key size for Subordinate CA certificates listed in Appendix A of the CAB Forum Baseline Requirements, which can be found at https://www.cabforum.org.

11. New Intermediate CA certificates under root certificates submitted for distribution by the Program must separate Server Authentication Code Signing and Time Stamping uses. This means that a single issuing CA must not be used to issue both server authentication and code signing certificates. A separate CA must be used for each use case. Please note that this requirement does not apply to roots enrolled in the Program prior to July 1, 2015.

12. Rollover root certificates, or certificates which are intended to replace previously enrolled but expired certificates, will not be accepted if they combine server authentication with code signing uses unless the uses are separated by application of Extended Key Uses ("EKU"s) at the intermediate CA certificate level that are reflected in the whole certificate chain.

13. End-entity certificates must meet the requirements for algorithm type and key size for Subscriber certificates listed Section 6.1.5 ~~in Appendix A~~ of the CAB Forum Baseline Requirements located at https://cabforum.org/baseline-requirements-documents/.

14. For Server Authentication certificates, Windows will stop ~~accepting~~ trusting SHA1 certificates by 1 January 2017. This means any SHA1 SSL certificates issued before or after this announcement must be replaced with a SHA2 family of certificates (excluding SHA-224) equivalent by January 1, 2017.

Note
Please note: Microsoft will not require CAs to replace SHA1 Server Authentication certificates but will no longer trust SHA1 certificates after this date.

15. CAs must use the following OIDs in the end-entity certificate: DV 2.23.140.1.2.1; OV 2.23.140.1.2.2; EV 2.23.140.1.1.; IV 2.23.140.1.2.3; EV Code Signing 2.23.140.1.3; Non-EV Code Signing 2.23.140.1.4.

16. End-entity certificates that include a Basic Constraints extension in accordance with IETF RFC 5280 must have the cA field set to FALSE and the pathLenConstraint field must be absent.

B. Key Requirements

Algorithm	All Uses Except for Code Signing and Time Stamping	Code Signing and Time Stamping Use
Digest Algorithms	SHA1 (may submit until January 1, 2016) SHA2 (SHA256, SHA384, SHA512)	SHA1 ~~(~~may submit until January 1, 2016~~)~~ SHA2 (SHA256, SHA384, SHA512)
RSA	2048	4096 (New roots only)
ECC / ECDSA	NIST P-256, P-384, P-521	NIST P-256, P-384, P-521

C. Revocation Requirements

1. The CA must have a documented revocation policy and must have the ability to revoke any certificate it issues.

2. Deleted July 2015.

3. CAs that issue Server Authentication certificates must support the following OCSP responder requirements:

    a. Minimum validity of eight (8) hours; Maximum validity of seven (7)~~2~~ days; and

    b. The next update must be available at ~~-~~least eight (8) hours before the current period expires. If the validity is more than 16 hours, then the next update must be available at ½ of the validity period.

4. All certificates issued from a root certificate must support either the CRL distribution point extension and/or AIA containing an OCSP responder URL.

5. The CA must not use the root certificate to issue end-entity certificates.

6. If a CA issues Code Signing certificates, it must use a Time Stamp Authority that complies with RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)."

D. Code Signing Root Certificate Requirements

1. Qualifying for the code signing EKU. New root certificates submitted for distribution by the Program must be separate Server Authentication from EV Code Signing and Time Stamping uses at the intermediate certificate level.

2. New code signing root certificates must support the SHA2 hash algorithm.

3. Root certificates that support code signing use will be removed from distribution by the Program 10 years from the date of distribution of a replacement rollover root certificate, or a shorter deadline on request of the CA.

4. Root certificates that remain in distribution to support only code signing use beyond their algorithm security lifetime (e.g. RSA 1024 = 2014, RSA 2048 = 2030) will be limited to code signing use only.

5. Root certificates will be removed from distribution by the Program without regard to any unexpired end entity certificates issued from them, according to the following deadlines:

    a) Server Authentication certificates: CAs must begin issuing new certificates using only the SHA-2 algorithm after January 1, 2016. Windows will no longer trust certificates signed with SHA-1 after January 1, 2017.

    b) Code signing certificates: CAs must begin issuing new certificates using only the SHA-2 algorithm after January 1, 2016. For developers targeting Windows Vista and Server 2008 CAs will be allowed to continue issuing SHA-1 certificates.

    c) Time-stamping certificates: CAs must begin issuing new certificates using only the SHA-2 algorithm after January 1, 2016. For developers targeting Windows Vista and Server 2008, CAs will be allowed to continue issuing SHA-1 certificates. Windows will not enforce a policy on time-stamping certificates.

    d) OCSP signatures: Microsoft requires CAs to start issuing new OCSP signatures using only the SHA-2 algorithm after January 1, 2016. Windows will no longer trust OCSP responses that use SHA-1 for their signature if the corresponding certificate had the Must Stapleextension after January 1, 2016

    e) Time-stamp signature hashes: CAs must start issuing new time-stamp signature hashes using only the SHA-2 algorithm after January 1, 2016. For developers targeting Windows Vista and Server 2008, CAs will be allowed to continue issuing SHA-1 time-stamps.

E. EKU Requirements

1. CAs must provide a business justification for all of the EKUs assigned to their root certificate. Justification may be in the form of public evidence of a current business of issuing certificates of a type or types, or a business plan demonstrating an intention to issue those certificates in the near term (within one year of root certificate distribution by the Program).

2. Microsoft will only enable the following EKUs:

    a) Server Authentication =1.3.6.1.5.5.7.3.1

    b) Client Authentication =1.3.6.1.5.5.7.3.2

c) Secure E-mail EKU=1.3.6.1.5.5.7.3.4

d) Code Signing EKU=1.3.6.1.5.5.7.3.3

e) Time stamping EKU=1.3.6.1.5.5.7.3.8

f) Encrypting File System EKU=1.3.6.1.4.1.311.10.3.4

g) Document Signing EKU=1.3.6.1.4.1.311.10.3.12

F. Windows 10 Kernel Mode Code Signing (KMCS) Requirements

Windows 10 has heightened requirements to validate those kernel-mode drivers, which are appropriately signed by Microsoft and a Program partner. Partners who wish to become authorized for this program must complete the steps below.

1. The CA must send an email to trustcert@microsoft.com with:

2. Microsoft will evaluate whether the CA complies with all of the Program's requirements.
   a) A zipped copy of the .cer file of the root that the CA will use kernel-mode code signing; and
   b) The policy OID that the CA will use to identify kernel-mode code signing.

3. Microsoft will evaluate whether the CA complies with all of the Program's requirements.

4. Microsoft will send the CA the appropriate contract materials.

5. Upon receipt of the signed contract materials, Microsoft will add the partner to the list of authorized kernel-mode code signing partners.

5. Technical Best Practices

Though not required by Microsoft, the following represents what Microsoft believes to be the best practices that each CA should follow.

1. Microsoft recommends that each CA have an established communication channel to its customers. For example, if Microsoft were to notify the CA that Microsoft was disabling weak file hashes, the CA should have a method to notify its customers to use the updated signtool.exe file.

2. Because root certificates will be removed without regard to any unexpired end entity certificates issued from them, the CAs should plan to cease issuing end entity certificates for uses besides code signing such that those certificates expire according to these root removal guidelines.

3. While Windows will not enforce specific policies on Secure Email certificates, Microsoft recommends that CAs start issuing new Secure Email certificates using the SHA-2 algorithm.

4. Microsoft recommends an OCSP responder maximum validity period of one (1) day.

6. Security Incident Response Requirements

A. Definitions

1. "A compromise" means a direct or indirect incident, affecting either the CA or any of the CA's sub-roots o~~o~~r cross-signed, non-enrolled roots, that results in an actual or potential degradation of the security stature of the PKI, which includes hardware, software, or physical building issues.

2. "Security Incident" or "Incident" means any of the following that occur at the CA or a sub-CA:

    a) A Private Key compromise.

    b) A mis-issued certificate.

    c) A known or reasonably knowable, publicly reported compromise.

    d) Any physical compromise of the CAs infrastructure (e.g. physical access control failure, building compromise, or a failure of the HVAC in the data center).

    e) Any other issue that Microsoft identifies as calling into question the CA's integrity or trustworthiness.

3. "Exceptional Circumstance(s)" means an incident(s) in which Microsoft believes that the PKI is compromised; as to affect the security posture of a large number of Microsoft's customers.

B. Microsoft's Rights in the Event of an Incident

In the event of a Security Incident, Microsoft may at its sole discretion, do any of the following:

1. In an Exceptional Circumstance, immediately revoke any certificate the CA or any sub-CA has enrolled in the Program, otherwise it may revoke any certificate after providing seven days' notice to the CA.

2. Microsoft may take action including, but not limited to marking files signed by compromised certificates as malware, blocking web navigation to sites served with compromised Server Authentication certificates, preventing delivery of mail signed by compromised Secure Email certificates, etc.

3. Request that the CA make specific reports at a periodic interval to be determined by Microsoft.

4. Specify a due date for the CA to submit to Microsoft a final Security Incident report.

5. Communicate with affected third parties.

6. Require the CA to employ, at the CA's expense, a third-party investigator to investigate the Security Incident and prepare the final Security Incident report.

7. Disqualify any Qualifying Audit and require the CA to perform a new Qualifying Audit at the CA's sole expense.

C. Microsoft's Responsibilities in the Event of a Security Incident

In the event that Microsoft exercises any of the rights described above, Microsoft will:

1. Notify the CA, in writing, of its intentions 7 days prior to Microsoft's action, except under Exceptional Circumstances, in which case Microsoft will make reasonable efforts to communicate with the CA prior to taking action; and

2. Allow the CA to propose an alternate course of action, in which case, Microsoft will consider reasonable alternatives but reserves the right to reject such proposals if it deems the proposed course of action not to be in its customers' best interest.

D. CA Responsibilities in the Event of an Incident

In the event of a Security Incident, the CA must:

1. Notify Microsoft as soon as is practical but no later than 24 hours from the time of the Security Incident by (a) completing the form located at http://aka.ms/rootnotify, and (b) sending the completed form to rootnotify@microsoft.com. The form requires the following information (if known at the time):

    a) Who detected the incident.

    b) If available, who perpetrated the incident.

    c) When the CA discovered the incident.

    d) Where the incident occurred.

    e) Which Roots and, if requested by Microsoft, end-user certificates, were affected by the incident.

    f) Which, if any, sub-CAs were affected.

g) What the CA believes to be the underlying cause of the incident.

h) What remedial measures the CA has taken or will take that the CA believes will address the underlying cause of the incident.

i) Any other information the CA believes to be appropriate.
j) Any other information Microsoft requested when it responded to the initial notification.

2. At Microsoft's request, the CA must provide a list of all certificates that were mis-issued as a result of the incident.

3. At Microsoft's request, the CA must provide Microsoft with periodic reports at an interval specified by Microsoft. If Microsoft does not make a specific request within 24 hours of an initial notification, the CA must provide reports to Microsoft as it discovers any new information.

4. The CA must provide a final Security Incident report to Microsoft that includes:

a) A list of certificates and domains involved in the breach.

b) How did the CA detect the incident? If the CA did not detect the breach, who did and why did the CA not detect?

c) If there was a mismatch in the reports over time, why?

d) Detailed description of the exploit.

e) Details about what infrastructure was compromised.

f) Details about how the infrastructure was compromised.

g) A detailed timeline of events.

h) The CA's interpretation of who perpetrated the breach.

i) Log files (appendix only).

j) Was the vulnerability detected by the CAs normal operation? If it was not, please explain why.

k) Was the vulnerability discovered in the most-recent audit? If yes, then provide information if the vulnerability was remediated. If the vulnerability was not remediated, please provide information about the reason for not doing so.

l) Was this vulnerability detected by the most-recent audit? If it was not, please explain why.

m) If the vulnerability was detected in the most recent audit, was it remediated? If not please explain why.

n) What changes to the CP/CPS policies will the CA make?
o) Detailed description of how the issue was closed.

5. If requested by Microsoft, a complete investigative and technical report of the compromise.