Apple Root Certificate Program

Program Requirements

Apple uses public key infrastructure (PKI) to secure and enhance the experience for Apple users. Apple products, including our web browser Safari and Mail.app, use a common store for root certificates. Apple requires root certification authorities to meet certain criteria, which include:

- Certification Authority (CA) providers must complete a WebTrust Principles and Criteria for Certification Authorities audit or equivalent.
- Transport Layer Security (TLS) CA providers must complete a WebTrust SSL Baseline Requirements Audit Criteria for Certification Authorities audit or equivalent and maintain compliance with the CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates.
- Extended Validation (EV) CA providers must complete a WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL audit or equivalent and maintain compliance with the CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates.
- CA providers must strictly limit the number of roots per CA provider.
- A root certificate must provide broad value to Apple's users.
- CA providers must demonstrate equivalence if submitting a non-WebTrust audit.
- CA providers must notify Apple if they anticipate a change in control. Do not assume trust is transferable.

Submission Process

To begin the submission process, e-mail certificate-authority-program@apple.com requesting inclusion of your root certificate. CA providers will be contacted if any additional information is required, and when consideration of the inclusion request is complete.

Root Acceptance

Apple accepts and removes root certificates as it deems appropriate in its sole discretion.