Mozilla Root Program Update

June 6, 2023

Previous Presentation:
https://cabforum.org/wp-content/uploads/5-2023-February-Mozilla-Update-CABF-Ottawa-F2F.pdf

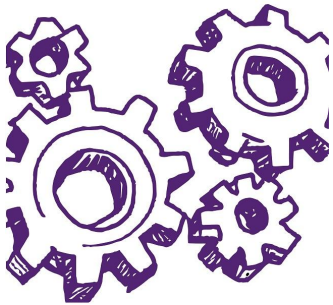
Ben Wilson and Kathleen Wilson
Mozilla Root Store Program Managers

Root Store Program Priorities

Protect user security and privacy and
Keep the web safe for our end users

Public, transparent processes
Community participation

Continual improvement,
Automation, and Agility



Information Gathered From:

	At Inclusion	Ongoing
Certification Practice Statements	✔	✔
Root Inclusion Considerations	✔	
Compliance Self-Assessments	✔	✔
Value-vs-Risk Justifications	✔	
Audit Reports	✔	✔
Incident Reporting	✔	✔

Root Inclusion Considerations

Goal: Help us make earlier, more objective decisions.

Unacceptable Behavior

Mozilla should deny root inclusion request.

Concerning Behavior

In aggregate may lead to denying the root inclusion request.

Warning Signs

CA operators must improve their operations and demonstrate their ability to maintain the higher level of operations, or their root inclusion request will be denied.

Please review **https://wiki.mozilla.org/CA/Root_Inclusion_Considerations**, and provide feedback on the Mozilla dev-security-policy list.

Process - Mozilla Root Store Policy (MRSP) v2.9

- Leverage the "issue" functionality in GitHub (complete)
- Select and "label" issues to resolve (complete)
- Announce issues to be discussed in MDSP (5/30/2023)
- Public discussions to determine specific language for MRSP (June 2023)
- Communication To CAs and Survey (June-July 2023)
- Adopt policy (before the end of July 2023)
- Publish policy (August 2023)

https://wiki.mozilla.org/CA/Updating_Root_Store_Policy

MRSP 2.9: Significant Changes

GitHub Issue #:

123 - Annual submission of Compliance Self-Assessments

https://wiki.mozilla.org/CA/Compliance_Self-Assessment

252 - Clarify requirements for reporting security incidents

232 - Reduced Useful Life for Root CAs

258 - Adopt S/MIME Baseline Requirements

MRSP 2.9: Reduce Useful Life for Root CAs

Key Material Created	Removal of Websites Trust Bit	Distrust for S/MIME After Date
Before 2006	April 15, 2025	April 15, 2028
2006-2007	April 15, 2026	April 15, 2029
2008-2009	April 15, 2027	April 15, 2030
2010-2011	April 15, 2028	April 15, 2031
2012- April 14, 2014	April 15, 2029	April 15, 2032
April 15, 2014 - present	15 years from creation	18 years from creation

Distrust Date

For TLS: Websites trust bit will be removed 15 years after CA key creation.
For Email: Mozilla will set “Distrust for S/MIME After Date” to 18 years from CA key creation.

CA Key Creation

Will be determined by the date in the auditor-witnessed key generation report.

https://wiki.mozilla.org/CA/Root_CA_Lifecycles

MRSP 2.9: Adopt S/MIME Baseline Requirements

- Certificates issued on or after 9/1/2023 capable of being used to digitally sign or encrypt email messages
- First S/MIME BR Audit dates to be discussed in MDSP
  - ETSI TS 119 411-6
  - WebTrust for CAs - S/MIME
- EdDSA Curve25519 and Curve448
- "Technically Constrained" must comply with § 7.1.5 (Name constraints) of S/MIME BRs

MRSP 2.9: Minor Changes

GitHub Issue #:

239 - Link to 5.1 of the CCADB Policy for audit letter requirements

250 - CCADB disclosure of unexpired, revoked CA certificates

254 - Harmonize CRL reason codes with Baseline Requirements

263 - Clarify what it means for a CP/CPS to follow RFC 3647

266 - Reference CCADB instructions for incident reporting

267 - Updated references to current Webtrust audit criteria

Contacting Us:

certificates@mozilla.org