S/MIME Certificate Working Group

April 10, 2024

Antitrust Compliance

CA/BROWSER FORUM

NOTE WELL

All participants are reminded that they must comply with the CA/Browser Forum's Bylaws, which include an antitrust policy, a code of conduct, and an intellectual property rights agreement.

Please contact the Forum Chair with any comments or concerns about the Bylaws or these policies

Agenda

CA/BROWSER FORUM

1. Roll Call
2. Note well: Antitrust / Compliance Statement
3. Review Agenda
4. Approval of past minutes
   - March 27
5. Discussion as time permits:
   - Ballot SMC06 is in Voting Period until April 11 https://lists.cabforum.org/pipermail/smcwg-public/2024-April/000957.html
   - Use of XX country code in Gov OrgID (Issue 240) https://github.com/cabforum/smime/issues/240
   - Discussion relating to Legacy profile deprecation (summary of differences between Legacy/Multi/Strict)
6. Any other business
   - Cancel May 22 meeting due to proximity to F2F# 62
7. Next meeting: Wednesday, April 24 2024 at 11:00 am Eastern Time

Legacy Approach

CA/BROWSER FORUM

- Legacy profiles were always intended as a stepping stone to facilitate moving S/MIME into an auditable regime
- The intent was always to eventually deprecate Legacy when appropriate
- Provide adequate time for Cert Issuers to identify blockers to migration
  - We believe the Multipurpose profiles still provide significant flexibility

- Multistep process
  - Identify if changes are required and, if so, define them
  - Ballot to introduce a deprecation date (and associated changes, if required)
  - Later, in a clean up ballot after the deprecation date, remove the Legacy references
    - Or, can we pre-approve that in this Ballot?

Legacy

CA/BROWSER FORUM

- See example profiles from PKIlint: https://github.com/digicert/smbr-cert-factory

- Differences exist in the Legacy vs Multi/Strict profiles
  - Validity period
  - Extensions: cRLDistributionPoints, authorityInformationAccess, id-ad-caIssuers, keyUsage, extKeyUsage, subjectDirectoryAttributes, and Adobe extensions
  - CRL reason
  - Allowed Subject DN attributes also vary

Validity Period

CA/BROWSER FORUM

https://github.com/cabforum/smime/blob/main/SBR.md#632-certificate-operational-periods-and-key-pair-usage-periods

- Legacy - 1185 days
- Multi/Strict - 825 days

Legacy Profiles

CA/BROWSER FORUM

https://github.com/cabforum/smime/blob/main/SBR.md#7123-subscriber-certificates

- cRLDistributionPoints: Multi/Strict - Mandatory CDP can only be http
- authorityInformationAccess: Multi/Strict - id-ad-ocsp and id-ad-caIssuers, if used, can only be http
- keyUsage: Strict - dataEncipherment goes away for rsaEncryption
- extKeyUsage: Strict - only emailProtection is allowed
- subjectDirectoryAttributes: Multi/Strict - not allowed
- Adobe extensions: Strict: not allowed

https://github.com/cabforum/smime/blob/main/SBR.md#722-crl-and-crl-entry-extensions

- Strict: Hold not allowed

Legacy Subjects

CA/BROWSER FORUM

https://github.com/cabforum/smime/blob/main/SBR.md#71423-subject-dn-attributes-for-mailbox-validated-profile

- 7.1.4.2.3 - mailbox - no difference
- 7.1.4.2.4 - org
  - Multi - Other not allowed
  - Strict - streetAddress, postalCode, Other not allowed
- 7.1.4.2.5 - sponsor
  - Multi/Strict SHALL include either subject:givenName and/or subject:surname, or the subject:pseudonym
  - Multi - Other not allowed
  - Strict - streetAddress, postalCode, Other not allowed
- 7.1.4.2.6 - individual
  - Multi/Strict SHALL include either subject:givenName and/or subject:surname, or the subject:pseudonym
  - Multi - Other not allowed
  - Strict - streetAddress, postalCode, Other not allowed