S/MIME Certificate Working Group

April 26, 2023

Antitrust Compliance

CA/BROWSER FORUM

NOTE WELL

All participants are reminded that they must comply with the CA/Browser Forum anti-trust policy, code of conduct, and intellectual property rights agreement which can be found in Section 1.3 of the Bylaws and cabforum.org.

Please contact the chair with any comments or concerns about these policies

Agenda

CA/BROWSER FORUM

1. Roll Call
2. Note well: Antitrust / Compliance Statement
3. Review Agenda
4. Approval of past minutes
   -April 12

5. Discussion

   a) Linting
   b) Review of Christophe's Pseudonym fix
   https://github.com/srdavidson/smime/commit/fc91ff14449f7d2cdee630e1e5167695baa3d186
   c) Review of LEI role clarification
   https://github.com/srdavidson/smime/commit/9966e8b1ad777df4cb1bf455482bb08e654243e6
   d) Discussion of Enterprise RA: issuing certificates to external email domains using "3.2.2.2 Validating control over mailbox via email"

6. Any other business
7. Next call: Wednesday, May 10, 2023 at 11:00 am Eastern Time
   Adjourn

ERA thinking

Question being posed:

Why can’t an ERA combine an external mailbox with their own O details?

Background behind the way the S/MIME BR were written:

- Currently ERA may only issue “identity profiles” to domains they control or are authorised to use
  - The idea is that an ERA can reliably “sponsor” internal users
  - Therefore simple delegation of RA
- Users on external mail domains are harder to scope for RA
  - Therefore ERA use the Mailbox-validated profile, without identity information
  - Does the external mailbox “belong to” the cert individual Subject … or whoever “owns” the email domain? The email domain owner may not want their email in a cert issued by/naming another O.

ERA - Current Text

CA/BROWSER FORUM

1.3.2.1 Enterprise registration authorities

The CA MAY delegate to an Enterprise Registration Authority (RA) to verify Certificate Requests from the Enterprise RA's own organization. The CA SHALL NOT accept Certificate Requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. If the Certificate Request is for an `Organization-validated` or `Sponsor-validated` profile, the CA SHALL confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with Section 3.2.2.1 or Section 3.2.2.3. The CA SHALL confirm that the `subject:organizationName` name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are Affiliated as defined in Section 3.2 or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested email domain falls within the subdomains of ABC Co.'s Registered Domain Name.
2. If the Certificate Request is for a `Mailbox-validated` profile, the CA SHALL confirm that the mailbox holder has control of the requested Mailbox Address(es) in accordance with Section 3.2.2.2.

The CA SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA in accordance with Section 8.8.

ERA - Proposed Update Text

CA/BROWSER FORUM

1.3.2.1 Enterprise registration authorities

The CA MAY delegate to an Enterprise Registration Authority (RA) to verify Certificate Requests for Subjects within the Enterprise RA's own organization. The CA SHALL NOT accept Certificate Requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. If the Certificate Request is for a `Mailbox-validated`, `Organization-validated`, or `Sponsor-validated` profile, the CA SHALL confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with Section 3.2.2.1 or Section 3.2.2.3.
2. The CA SHALL confirm that the `subject:organizationName` name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are Affiliated as defined in Section 3.2 or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested email domain falls within the subdomains of ABC Co.'s Registered Domain Name.

The CA SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA in accordance with Section 8.8.

An Enterprise RA MAY also submit Certificate Requests using the `Mailbox-validated` profile for users whose email domain(s) are not under the delegated organization’s authorization or control. In this case, the CA SHALL confirm that the mailbox holder has control of the requested Mailbox Address(es) in accordance with Section 3.2.2.2.