CAB CA/BROWSER FORUM

S/MIME Certificate Working Group

Face to Face, February 22, 2022

SMCWG

CA/BROWSER FORUM

Chair: Stephen Davidson
Vice Chair: Mads Henriksveen

29 Certificate Issuers

AC Camerfirma, Actalis, Asseco Data Systems (Certum), BuyPass, CFCA, Chunghwa Telecom, Comsign, DigiCert, D-TRUST, eMudhra, Entrust, GDCA, GlobalSign, GlobalTrust, HARICA, Identrust, iTrusChina,
MSC Trustgate.com, SecureTrust, SECOM Trust Systems, Sectigo, SHECA, SSC, SSL.com, SwissSign, Telia, TrustCor, TWCA, OISTE Foundation

6 Certificate Consumers

Apple, Google, Microsoft, Mozilla/Thunderbird, runQuadrat, Zertificon

4 Associate Members

ACAB Council, tScheme, US Federal PKI, WebTrust

5 Interested Parties

Arno Fiedler, PSW, TeleTrusT, Vigil Security, Nathalie Weiler

Charter

CA/BROWSER FORUM

The SMCWG is chartered to work on requirements applicable to CAs that issue S/MIME certificates used to sign, verify, encrypt, and decrypt email.

Certificate profiles for S/MIME certificates and Issuing CA certificates
Verification of control over email addresses
Key management, certificate lifecycle, etc.
CA operational practices, physical/logical security, etc.
Identity validation for natural persons and legal entities

Where possible, to leverage work already undertaken by other CABF groups.

2021 Recap

CA/BROWSER FORUM

Ongoing drafting is transparent at https://github.com/cabforum/smime/blob/preSBR/SBR.md

Walk thru of relevant standards

Discussion of S/MIME use cases and user types

Definition of Certificate Profiles

- Types: Mailbox, Organization, Sponsored, Individual
- Tiers: Legacy, Multipurpose, Strict
- Target validity periods

Discussion re CA settings and algorithms

Support for draft-ito-documentsigning-eku-00 for eventual separation of S/MIME from document signing

Discussion of suitable methods for:

- Organization vetting
- Mailbox control

2022 Targets

CA/BROWSER FORUM

Discussion of:

- OrganizationIdentifier
- Enterprise RA
- Individual vetting (based upon methods in CS BR and in ETSI TS 119 461)
- Archive and escrow

Resolve outstanding questions regarding Organization vetting (legal existence)

Review adequacy of “pickup” sections from TLS BR
Survey remaining gaps in draft S/MIME BR

Ongoing collation of issues for later versions

> Complete drafting of S/MIME BR

Roadmap to a ballot

- Define approach to review draft, address comments

Comments:

- BR of BR – frequently used sections
- Style guide
- Standard for cross-inclusions
- EV in RFC 3647

CAB CA/BROWSER FORUM

S/MIME Certificate Working Group

February 24, 2022

Antitrust Compliance

CAB CA/BROWSER FORUM

“As you know, this meeting includes companies that compete against one another. This meeting is intended to discuss technical standards related to the provision of existing and new types of digital certificates without restricting competition in developing and marketing such certificates. This meeting is not intended to share competitively-sensitive information among competitors, and therefore all participants agree not to discuss or exchange information related to:

1. Pricing policies, pricing formulas, prices or other terms of sale;
2. Costs, cost structures, profit margins,
3. Pending or planned service offerings,
4. Customers, business, or marketing plans; or
5. The allocation of customers, territories, or products in any way.”

F2F Agenda Topics

Requirements for Enterprise RA
(section 1.3.2 and 8.8)

Initial proposal for Individual vetting
(section 3.2.4)

Roadmap to a ballot

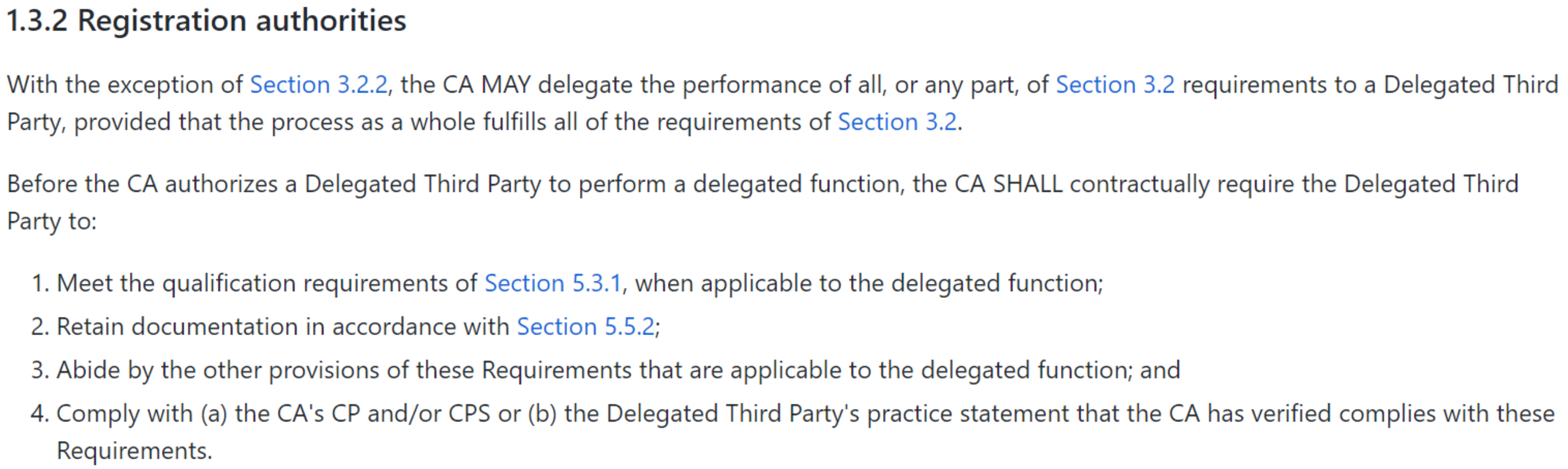
Enterprise RA

- Responsible for majority of S/MIME
- Clarify the division between Enterprise RA (internal) and Delegated Third Party RA (external)

Enterprise RA:

- Can issue to internal users via Organisation-validated and Sponsor-validated profiles
    - Constrained to Subject and email domains
    - Use of mailbox control method??
- Can still issue to external users via Mailbox-validated profile
    - Use of mailbox control method
- Authoritative source for Individual Identity in Sponsor-validated profile

Delegated RA



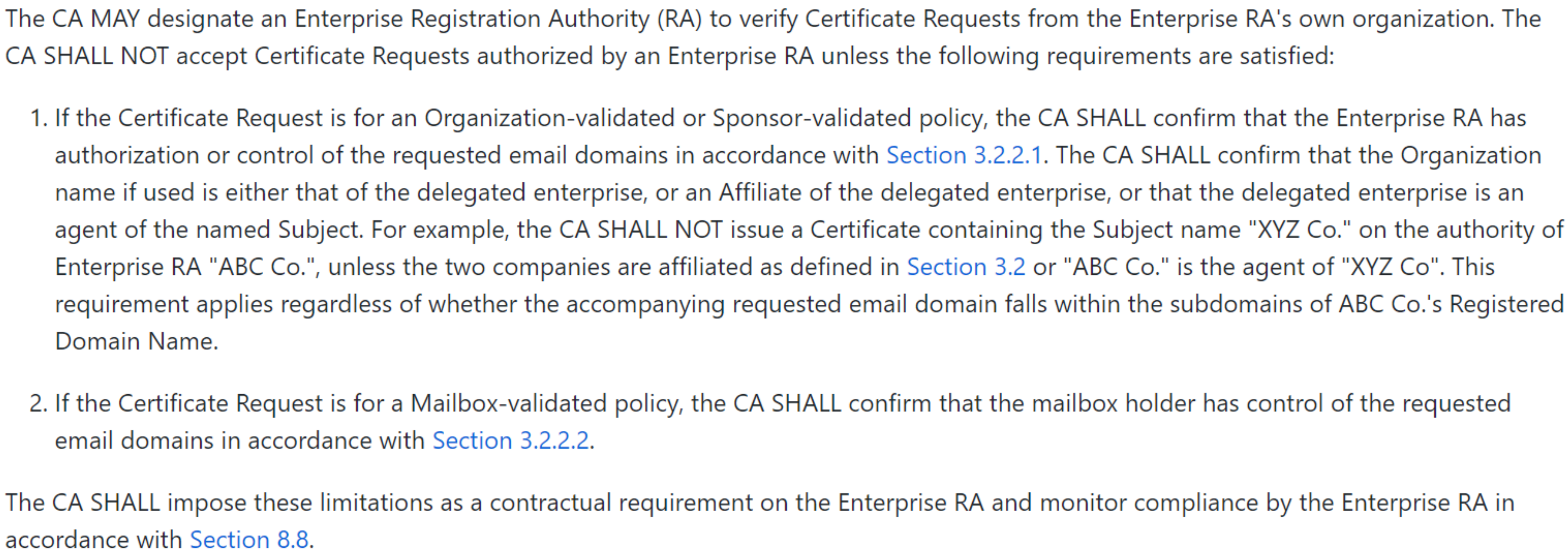
1.3.2 Registration authorities

With the exception of Section 3.2.2, the CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2.

Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA SHALL contractually require the Delegated Third Party to:

1. Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function;
2. Retain documentation in accordance with Section 5.5.2;
3. Abide by the other provisions of these Requirements that are applicable to the delegated function; and
4. Comply with (a) the CA's CP and/or CPS or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.

Enterprise RA



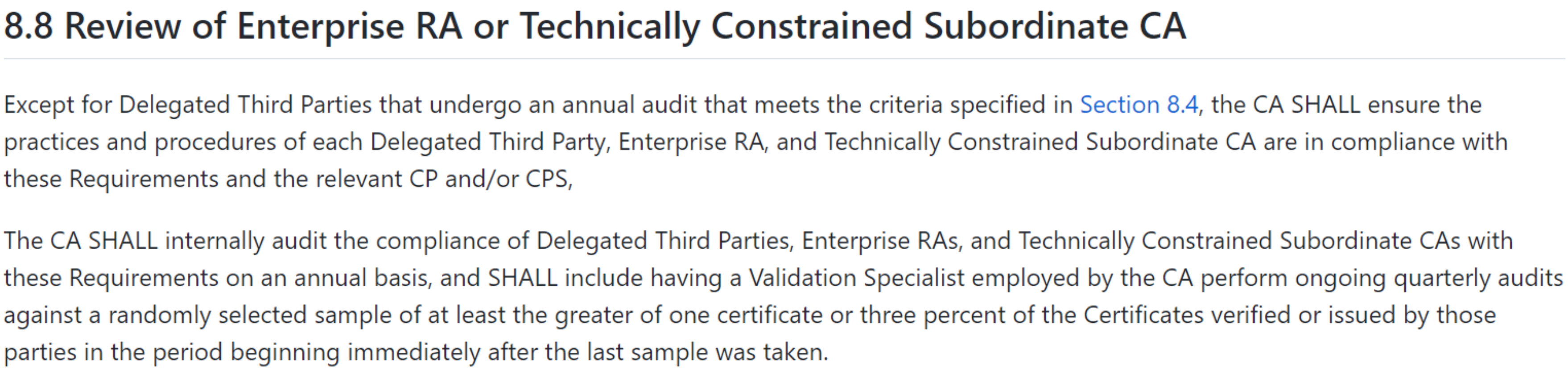
The CA MAY designate an Enterprise Registration Authority (RA) to verify Certificate Requests from the Enterprise RA's own organization. The CA SHALL NOT accept Certificate Requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. If the Certificate Request is for an Organization-validated or Sponsor-validated policy, the CA SHALL confirm that the Enterprise RA has authorization or control of the requested email domains in accordance with Section 3.2.2.1. The CA SHALL confirm that the Organization name if used 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 policy, the CA SHALL confirm that the mailbox holder has control of the requested email domains 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.

Enterprise RA

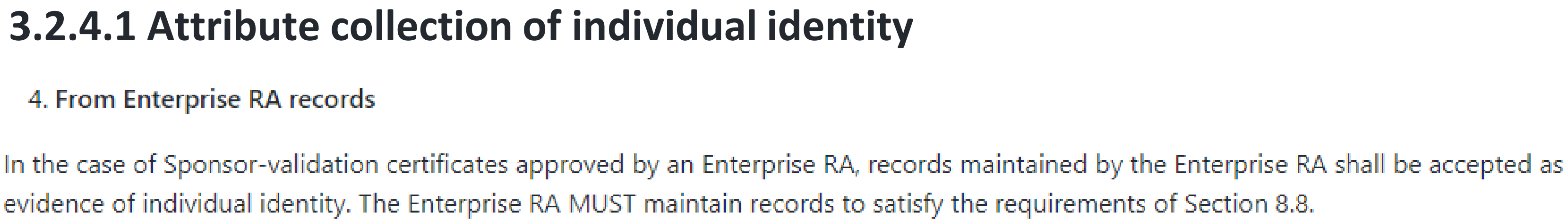


8.8 Review of Enterprise RA or Technically Constrained Subordinate CA

Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.4, the CA SHALL ensure the practices and procedures of each Delegated Third Party, Enterprise RA, and Technically Constrained Subordinate CA are in compliance with these Requirements and the relevant CP and/or CPS,

The CA SHALL internally audit the compliance of Delegated Third Parties, Enterprise RAs, and Technically Constrained Subordinate CAs with these Requirements on an annual basis, and SHALL include having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified or issued by those parties in the period beginning immediately after the last sample was taken.

Enterprise RA



3.2.4.1 Attribute collection of individual identity

4. From Enterprise RA records

In the case of Sponsor-validation certificates approved by an Enterprise RA, records maintained by the Enterprise RA shall be accepted as evidence of individual identity. The Enterprise RA MUST maintain records to satisfy the requirements of Section 8.8.

Individual Identity

Responsible for majority of S/MIME

Clarify the division between Enterprise RA (internal) and Delegated Third Party RA (external)

Lay out requirements for different methods:

- From a physical identity document
- From a digital identity document
- From a certificate supporting a digital signature applied by the Applicant
- From Enterprise RA records
- Use of authorized reference sources for supplementary evidence
- Use of Verified Professional Letter

Draw upon CS BR and ETSI TS 119 461 (identity proofing)

Roadmap to Ballot

Complete gap analysis of existing draft
Resolve open questions
Agree parked items for v1.1

Draft text of S/MIME BR
Comment period

- How to orchestrate review, resolution

Ballot
Effective date(s)
Audit criteria
Fade out of Legacy profile
WG Officers – Oct 31, 2022

Roadmap to Ballot

5.1. Voting Structure

The rules described in Bylaw 2.3 and 2.4 SHALL apply to all ballots, including Draft Guideline Ballots.

In order for a ballot to be adopted by the SMCWG, two-thirds or more of the votes cast by the Certificate Issuers must be in favor of the ballot and more than 50% of the votes cast by the Certificate Consumers must be in favor of the ballot. At least one member of each class must vote in favor of a ballot for it to be adopted. Quorum is the average number of Member organizations (cumulative, regardless of Class) that have participated in the previous three (3) SMCWG Meetings or Teleconferences (not counting subcommittee meetings thereof). No Ballots shall be adopted until at least (3) meetings have occurred and quorum determined.

- Endorsers
- Final draft ballot – 7 day discussion
- Vote – 7 day vote
- IPR review – 60 day