The following text enacts the MozPol requirements in:

For a certificate capable of being used for digitally signing or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate or has been authorized by the email account holder to act on the account holder's behalf. The CA SHALL NOT delegate validation of the domain portion of an email address. The CA MAY rely on validation the CA has performed for an Authorization Domain Name (as specified in the Baseline Requirements) as being valid for subdomains of that Authorization Domain Name. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs to perform this verification.

3.2.2 Authentication of organization and domain identity

3.2.2.1 Authentication of organization identity

TBD

3.2.2.2 Validation of domain authorization or control

This section defines the permitted processes and procedures for confirming the Applicant's control of the email addresses to be included in issued Certificates.

The CA MUST verify that Applicant controls the email accounts associated with all email addresses referenced in the Certificate or has been authorized by the email account holder to act on the account holder's behalf using one of the methods described in this Section.

Note: Email addresses may be listed in Subscriber Certificates using Rfc822Names in the subjectAltName extension or in Subordinate CA Certificates via Rfc822Names in permittedSubtrees within the Name Constraints extension.

The CA's CP/CPS MUST specify the procedures that the CA employs to perform this verification. CAs SHALL maintain a record of which domain validation method, including relevant BR or SBR version number, used to validate every domain or email address in issued Certificates.

3.2.2.2.1 Validating authority over email address via domain

Confirming the Applicant has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the email address to be used in the Certificate.

The CA SHALL only use the approved methods in Section 3.2.2.4 of Version 1.7.3 of the BR to perform this verification

The CA SHALL NOT delegate validation of the domain portion of an email address.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance.

For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

3.2.2.2.2 Validating control over email address via email

Confirming the Applicant's control over the email address by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent only to the address being validated and SHALL not be shared in any other way.

The Random Value SHALL be unique in each email.

The CA MAY resend the email in its entirety, including re-use of the Random Value, provided that the entire contents and recipient email address of the communication remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Completed validations of Applicant control over the email address must be performed for each Certificate issuance.

3.2.2.3 CAA Records

TBD