**S/MIME Certificate Working Group (SMCWG) Charter**

**Introduction**

This introduction provides general information and context with an intent to assist the interpretation of this Charter.

An S/MIME certificate contains the public key bound to an email address and may also contain the identity of a natural person or legal entity that controls such email address. The key pair can then be used to sign, encrypt and decrypt email. An S/MIME certificate can be identified by the existence of an Extended Key Usage (EKU) Object Identifier (OID) of 1.3.6.1.5.5.7.3.4 for emailProtection.

The objective of an S/MIME certificate is to provide cryptographic security services for electronic messaging applications, namely sender authentication, message integrity, and message privacy through encryption. For effective authentication and privacy, it is imperative that the CA validates the subject’s identity (if present) and its email address. The recipient of a digitally signed message can authenticate an email message to receive protection against email spoofing and can encrypt a response to the orginal sender by referring to the public key, email address, and distinguished name (if present) contained in an S/MIME certificate.

The primary use case under consideration for the working group is a model whereby senders and recipients of email messages receive “reasonable assurance” that the other party to the communication identified in the certificate has control of the domain or email address being asserted. A variation of this primary use case is where an individual or organization digitally signs email to establish its authenticity and source of origin.

Therefore, in order to provide reasonable assurance, it is crucial to establish a standard method to validate an email address and the subject’s identity (if present) prior to binding them to the public key. “Reasonable assurance” is to be determined and defined by this SMCWG through studying the existing methods that exist in the industry, as well as identity management frameworks and any applicable legislation.

An S/MIME certificate can also be used in an automated message with transfer agents that use cryptographic security services that do not require any human intervention, such as the signing of software-generated documents and the encryption of fax messages sent over the Internet. While these existing use cases are not in scope for the SMCWG, care will be exercised by the SMCWG to avoid unintended adverse effects to these uses. The security, stability and resiliency of the Internet shall be taken into consideration when the SMCWG forms its consensus. The SMCWG will consult other technical communities when and as necessary.

The problem to be addressed by the working group is the absence of consistent and audited validation practices used by CAs in establishing the identity of the subject (if present) and verifying that the subscriber controls the email address. While there are methods for validating control of a domain that can be adopted from TLS certificates, there are currently no standard requirements for validating control of email addresses. Methods for validating identities in TLS certificates also exist and should be leveraged where possible, as well as other identity validation standards common in the industry (e.g. European standards). A method to efficiently validate an email address as well as developing a consistent profile for S/MIME certificates in order to facilitate technical interoperability across the Internet is also to be addressed by the SMCWG.

**Chartering of the S/MIME Certificate Working Group**

A Chartered Working Group (“SMCWG”) is created to perform the activities as specified in this Charter, subject to the terms and conditions of the CA/Browser Forum Bylaws and Intellectual Property Rights (IPR) Policy, as such documents may change from time to time. This charter for the S/MIME Certificate Working Group has been created according to CAB Forum Bylaw 5.3.1. In the event of a conflict between this Charter and any provision in either the Bylaws or the IPR Policy, the provision in the Bylaws or IPR Policy SHALL take precedence. The definitions found in the Forum’s Bylaws SHALL apply to capitalized terms in this Charter.

1. Scope

The authorized scope of the SMCWG SHALL be to discuss, adopt, and maintain policies, frameworks, and sets of standards related to the issuance and management of S/MIME certificates by third-party CAs under a publicly trusted root, limited as follows:

(a) Baseline verification of control over email addresses, including those used by a natural person or a legal entity, or used by automated systems such as for mailing lists

(b) Identity validation for natural persons and legal entities

(c) Key management and certificate lifecycle (subject to coordination with other Forum CWGs to ensure consistency and avoid redundancy)

(d) Certificate profiles for S/MIME certificates and Issuing CA certificates (including the appropriateness of extensions and when those extensions should be present)

(e) CA operational practices, physical/logical security, etc.

The SMCWG SHALL exercise caution to ensure that its work product does not impede the issuance of certificates with other EKU types.

1. Out of Scope

Certificates issued under a root certificate that is not publicly trusted SHALL be out of scope.

1. Charter Expiration

The SMCWG is chartered indefinitely until it is dissolved as specified in Bylaw 5.3.2(c).

1. Personnel and Participation

4.1. Selection of Officers

Stephen Davidson will act as chair of the SMCWG until the first Working Group Teleconference, at which time the group will elect a chair and vice-chair. The chair and vice-chair will serve until October 31, 2020, or until they are replaced, resign, or are otherwise disqualified. Thereafter, elections SHALL be held for chair and vice chair every two years in coordination with the Forum’s election process and in conjunction with its election cycle. Voting SHALL occur in accordance with Bylaw 4.1(c).

4.2. Participation

4.2.1. Eligibility to Participate, Suspension, and Termination of Membership in SMCWG

The SMCWG SHALL consist of two classes of voting members, Certificate Issuers and Certificate Consumers meeting the eligibility criteria below.

(1) A Certificate Issuer eligible for voting membership in the SMCWG MUST have a publicly-available audit report or attestation statement in accordance with one of the following schemes:

* WebTrust for CAs v.2.0 or newer; or
* ETSI EN 319 411-1, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied); or
* If a Government Certificate Issuer is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review.

These audit reports must also meet the following requirements:

* They must report on the operational effectiveness of controls for a historic period of at least 60 days;
* No more than 27 months have elapsed since the beginning of the reported-on period and no more than 15 months since the end of the reported-on period; and
* The audit report was prepared by a Qualified Auditor.

In addition, the Certificate Issuer MUST actively issue S/MIME certificates that are treated as valid by Certificate Consumers that produce a mail user agent, mail transfer agent, or email service provider that implements S/MIME features.

(2) A Certificate Consumer eligible for voting membership in the SMCWG must produce, develop and maintain a mail user agent (web-based or application based), mail transfer agent, or email service provider that processes S/MIME certificates issued by third-party Certificate Issuers who meet criteria set by such Certificate Consumer.

The Working Group SHALL allow participation by Interested Parties, as set forth in the Bylaws.

4.2.2. Membership Application/Declaration Process

A. An Applicant not already a member of the Forum SHALL provide the following information:

* Confirmation that the applicant satisfies at least one (1) of the membership eligibility criteria (and if it satisfies more than one (1), indication of the single category under which the applicant wishes to apply).
* The organization name, as they wish it to appear on the Forum Web site and in official Forum documents.
* URL of the applicant’s main Web site.
* Names and email addresses of employees who will participate in the Working Group and Forum as Member representatives.
* Emergency contact information for security issues related to certificate trust.

Applicants that qualify as Certificate Issuers or Root Certificate Issuers must supply the following additional information:

* URL of the current qualifying audit report.
* Links or references to issued end-entity certificates that demonstrate them being treated as valid by a Certificate Consumer Member.

Such Applicant SHALL become a Member once the SMCWG has determined by consensus among the Members during a SMCWG Meeting or Teleconference that the Applicant meets all of the requirements above or, upon the request of any Member of the SMCWG, by a Ballot among Members of the SMCWG. Acceptance by consensus shall be determined or a Ballot of the Members shall be held as soon as the Applicant indicates that it has presented all information required above and has responded to all follow-up questions from the SMCWG and the Member has complied with the requirements of Bylaw 5.5.

Certificate Issuer applicants that are not actively issuing S/MIME certificates but otherwise meet these membership criteria MAY request to the SMCWG that they be granted an invitation for Associate Member status in accordance with Bylaw 3.1, subject to conditions designated by the SMCWG.

The SMCWG SHALL allow participation by Interested Parties, as set forth in the Bylaws.

B. Existing CAB Forum Members seeking to participate in the SMCWG, in accordance to Bylaw 5.3.1(c), MUST formally declare their intent to participate in writing and provide the SMCWG Chair with this declaration and evidence that they meet the criteria set forth above. Such Applicants SHALL become Members of the SMCWG as determined by consensus during a SMCWG Meeting or Teleconference, or upon the request of any Member of the SMCWG, by a Ballot among Members of the SMCWG.

In order to determine the composition of the initial set of SMCWG Members, at least twenty-four (24) hours prior to the initial meeting of the SMCWG, the SMCWG Chair SHALL publish a list of Members seeking to participate who he determines meet the criteria set forth above. As the first order of business at the first meeting of the SMCWG, those organizations on the Chair’s list of proposed, qualifying Members SHALL vote to determine the initial set of SMCWG Members.

The Chair of the SMCWG SHALL establish a list for declarations of participation and manage it in accordance with the Bylaws, the IPR Policy, and the IPR Policy Agreement.

4.2.3. Ending Working Group Membership

Members may resign from the SMCWG at any time. Resignation or other termination of membership in the SMCWG does not prevent a Member from potentially having continuing obligations, under the Forum’s IPR Policy or any other document.

A Certificate Consumer Member’s membership will automatically cease if any of the following become true:

1. it stops providing updates for its membership-qualifying software product; and
2. six (6) months have elapsed since the last such published update.

A Certificate Issuer’s membership in the SMCWG may be suspended if any of the following become true:

1. it fails to perform and disclose its membership-qualifying audit and fifteen (15) months have elapsed since the end of the audit period of its last successful membership-qualifying audit;
2. its membership-qualifying audit is revoked, rescinded or withdrawn;
3. fifteen (15) months have elapsed since the end of the audit period of its last successful membership-qualifying audit; or
4. it is no longer the case that its currently-issued certificates are treated as valid by at least one Certificate Consumer Member of the SMCWG.

Any Member who believes one of the above circumstances is true of any other Member may report it on the SMCWG’s Public Mail List. The SMCWG Chair will then investigate, including asking the reported Member for an explanation or appropriate documentation. If evidence of continued qualification for membership is not forthcoming from the reported Member within five (5) working days, the SMCWG Chair will announce that such Member is suspended, such announcement to include the basis upon which the suspension has been made.

A suspended Member who believes it has then re-met the membership criteria under the relevant clauses shall post its evidence to the SMCWG Public Mail List or provide evidence to the SMCWG Chair who SHALL post it to the SMCWG Public Mail List. The SMCWG Chair will examine the evidence and unsuspend the member, or not, by announcement to the SMCWG Public Mail List. A Member’s membership will automatically cease six months after it becomes suspended if the Member has not re-met the membership criteria by that time.

While suspended, a Member may participate in SMCWG Meetings, SMCWG Teleconferences, and on the SMCWG’s discussion lists, but may not propose or endorse ballots or take part in any form of voting.

Votes cast before the announcement of a Member’s suspension will stand.

1. Membership Declaration

In accordance with the IPR Policy, Members that choose to participate in the SMCWG MUST declare their participation and SHALL do so prior to participating. The Chair of the SMCWG SHALL establish a list for declarations of participation and manage it in accordance with the Bylaws, the IPR Policy, and the IPR Agreement.

6. Voting and Other Organizational Matters

6.1 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). For transition purposes, if three (3) meetings have not yet occurred, quorum is three (3).

6.2 Other Organizational Matters

(a) The Chair MAY delegate any of his/her duties to the Vice Chair as necessary. The Vice Chair has the authority of the Chair in the event of any absence or unavailability of the Chair, and in such circumstances, any duty delegated to the Chair herein MAY be performed by the Vice Chair. For example, the Vice Chair MAY preside at SMCWG Meetings and Teleconferences in the Chair’s absence.

(b) SMCWG-created Subcommittees MAY be approved either (1) by formal ballot as described in 5.1, or (2) by simple majority vote of those members present at a regularly scheduled SMCWG Meeting or Teleconference provided that the proposal is mentioned in an agenda circulated on the SMCWG Mail List at least forty-eight (48) hours prior to the SMCWG Meeting or Teleconference.

7. Summary of Major Deliverables

The deliverables of the SMCWG are defined in the Scope section above and shall be named the "Baseline Requirements for S/MIME Certificates" proposed standard.

8. Primary Means of Communication

(a) The SMCWG SHALL appoint a webmaster to maintain the SMCWG’s pages on the wiki and the Forum’s Public Web Site.

(b) The SMCWG will communicate primarily through listserv-based email in accordance with Bylaw 5.3.1(d). The SMCWG List SHALL be available to the public, who will not have posting privileges (i.e. anyone may subscribe to receive messages and the list may be crawled and indexed by Internet search engines).

(c) The SMCWG shall conduct periodic calls or face-to-face meetings as needed. Minutes SHALL be kept, and such minutes SHALL be made public in accordance with Bylaw 5.2.

9. IPR Policy

As with all Forum Working Group activity, the IPR Policy, v1.3 or later, SHALL apply to all activities and work of the SMCWG. All Participants in the SMCWG SHALL have on file with the Forum a valid, signed IPR Policy Agreement (v.1.3). A previously submitted IPR Policy Agreement (v1.3) by an existing Member of the Forum shall suffice as meeting the obligation under section 4.5 of the IPR Policy that a Participant in the SMCWG commit to CAB Forum License requirements.

In accordance with the Forum’s antitrust policy, an antitrust compliance statement SHALL be read at the start of all Working Group Meetings, in substantially the form written in Bylaw 1.3.