Ballot FORUM-8: Charter to Establish a Code Signing Certificate Working Group

Purpose of Ballot

It is proposed that the Forum establish a working group to adopt and maintain a policy, framework, and set of standards related to the issuance and management of code signing certificates by a third-party Certificate Issuer, rather than by the platform supplier (i.e. Certificate Consumer) itself. The work would be based on the Forum's prior adoption of the EV Code Signing Guidelines, version 1.4, (Ballot 172; 5 July 2016), and additional work by Forum members who expressly agreed to operate pursuant to the Forum's IPR Policy, between 2013 and 2015, which resulted in a failed proposal to adopt a set of baseline requirements for the issuance and management of code signing certificates (https://cabforum.org/wp-content/uploads/Code-Signing-Requirements-2015-11-19.pdf; https://cabforum.org/2015/12/17/ballot-158).

It is proposed by Ben Wilson of DigiCert and endorsed by Mike Reilly of Microsoft and Bruce Morton of Entrust Datacard that the Forum charter a working group to operate in accordance with the Scope and other provisions that follow. This Charter will take effect upon approval of the CAB Forum by ballot conducted in accordance with Bylaw 5.3.

— BALLOT BEGINS —

Code Signing Certificate Working Group Charter

Introduction

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

A code signing certificate contains the public key corresponding to a private key that is used by a person or organization to digitally sign data—such data usually containing instructions (i.e. "code") for hardware to perform certain tasks. A code signing certificate can be identified by the existence of an Extended Key Usage (EKU) Object Identifier (OID) of 1.3.6.1.5.5.7.3.3.

The objective of a code signing certificate is to provide a cryptographic way to identify the source of code. There are a variety of functional models and use cases whereby a code signing certificate is issued by a Certificate Issuer to a Subscriber for use in signing code that will run on a particular computing platform or group of platforms. (Each platform supplier determines how a chain between a trusted root CA certificate and the code signing certificate will be created and verified.)

The primary use case under consideration for the working group is a model whereby the platform supplier accepts code signing certificates issued by a third-party Certificate Issuer. A common example of this model is Microsoft's Authenticode, although others exist.

Other functional models include those which allow developers to self-sign code and those in which the platform supplier manages the code signing or certificate issuance process, and these models are expressly excluded from the working group's mandate. Common examples of these models that are expressly excluded from the scope of guidelines to be promulgated by the working group are Apple's Developer ID program and Google's Android.

Chartering of the Code Signing Certificate Working Group

Upon approval of the CAB Forum by ballot, the Code Signing Certificate Working Group ("CSCWG") 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. 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 CSCWG SHALL be to discuss, adopt, and maintain policies, frameworks, and sets of standards related to the issuance and management of code signing certificates by third-party Certificate Issuers under a publicly trusted root (and not code signing certificates issued under a private root CA), limited as follows:

a) EV Code Signing Guidelines, v. 1.4 and subsequent versions
b) Version 1.0 Draft of November 19, 2015, Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (subject to the CSCWG making a written finding that the provenance of such document is sufficiently covered by the Forum's IPR Policy)
c) Verification requirements for issuance/renewal of code signing certificates
d) Subscriber protection of private keys, including keys stored in the cloud
e) Certificate issuance and revocation
f) Requirements/controls on use of code signing certificates
g) Mechanisms to engage with AV vendors, researchers, and others regarding signed malware
h) Certificate profiles for code signing certificates and Issuing CA certificates (including the appropriateness of extensions and when those extensions should be present)
i) Certificate issuance and revocation
j) CA operational practices, physical/logical security, etc.

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

2 Out of Scope

The CSCWG SHALL NOT develop guidelines, standards, or requirements applicable to:

a) Self-signed code;
b) Platform suppliers / Certificate Consumers;
c) Certificates issued under a root certificate that is not publicly trusted, even though they are managed by Certificate Issuers or other third-party service providers; or
d) The code signing or certificate issuance process when managed by a platform supplier / Certificate Consumer.

3 Charter Expiration

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

4 Personnel and Participation

4.1 Selection of Officers

Dean Coclin will act as chair of the CSCWG until the first Working Group Teleconference, at which time the group will select 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 (2) years in coordination with the Forum's election process and in conjunction with its election cycle. Officer elections SHALL occur in accordance with Bylaw 4.1(c).

4.2 Eligibility to Participate, Suspension, and Termination of Membership in CSCWG

4.2.1 Eligibility to Participate

The CSCWG 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 CSCWG 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 code signing certificates that are accepted for use in computing platforms in which the platform supplier accepts code signing certificates issued by such Certificate Issuer.

(2) A Certificate Consumer (i.e. a platform supplier) eligible for voting membership in the CSCWG must produce a computing platform that accepts code signing certificates issued by third-party Certificate Issuers who meet criteria set by such Certificate Consumer.

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.
- The URL of at least one third party website that includes a certificate issued by the Applicant in the certificate chain.
- 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 CSCWG has determined by consensus among the Members during a CSCWG Meeting or Teleconference that the Applicant meets all of the requirements above or, upon the request of any Member of the CSCWG, by a Ballot among Members of the CSCWG. 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 CSCWG and the Member has complied with the requirements of Bylaw 5.5.

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

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

B. Existing CAB Forum Members seeking to participate in the CSCWG, in accordance to Bylaw 5.3.1(c), MUST formally declare their intent to participate in writing and provide the CSCWG Chair with this declaration and evidence that they meet the criteria set forth above.

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

Commented [DZ1]: Is the Chair alone supposed to evaluate each declaration?

4.2.3 Ending Working Group Membership

Members may resign from the CSCWG at any time. Resignation or other termination of membership in the CSCWG 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 CSCWG 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 CSCWG.

Any Member who believes one of the above circumstances is true of any other Member may report it on the CSCWG's Public Mail List. The CSCWG 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 CSCWG 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 CSCWG Public Mail List or provide evidence to the CSCWG Chair who SHALL post it to the CSCWG Public Mail List. The CSCWG Chair will examine the evidence and unsuspend the member, or not, by announcement to the CSCWG 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 CSCWG Meetings, CSCWG Teleconferences, and on the CSCWG'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.

5 Voting and Other Organizational Matters

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 Code Signing Certificates Working Group, 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) Code Signing Certificate Working Group Meetings or Teleconferences (not counting subcommittee meetings thereof). For transition purposes, if three (3) meetings have not yet occurred, quorum is three (3).

5.2 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 CSCWG Meetings and Teleconferences in the Chair's absence.

(b) CSCWG-created Subcommittees may be approved either (1) by formal ballot as described in Bylaw 2.3 or (2) by simple majority vote of those members present at a regularly scheduled CSCWG Meeting or Teleconference provided that the proposal is mentioned in an agenda circulated on the CSCWG Public Mail List at least twenty-four (24) hours prior to the CWG Meeting or Teleconference.

Commented [DZ2]: This seems a very short time to review and might "surprise" some members. I recommend removal.

6 Summary of Major Deliverables

The deliverables of the CSCWG are defined in the Scope section above.

7 Primary Means of Communication

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

(b) The CSCWG will communicate primarily through listserv-based email in accordance with Bylaw 5.3.1(d). The CSCWG 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 CSCWG 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.

8 IPR Policy and Antitrust Policy

As with all Forum Working Group activity, the IPR Policy, v1.3 or later, SHALL apply to all activities and work of the CSCWG. All Participants in the CSCWG 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 CSCWG 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.

--- MOTION ENDS---

The procedure for approval of this ballot is as follows:

Discussion Period (7+ days):

Start Time: Sunday, 17-February-2019 at 0100 UTC
End Time: Monday, 25-February-2019 at 1600 UTC

Vote for Approval (7 days):

Start Time: Monday, 25-February-2019 at 1600 UTC
End Time: Monday, 4-March-2019 at 1600 UTC