CA/BROWSER FORUM

CA/B Forum 2022-2024 (Update for F2F#61)

Plans - Strategy - Tasks

Issues with Bylaws - Charters

- Review and alignment of WG Charters
  - Divergence between Bylaws CWG template and other WGs (Elections, officers, **quorum**)
  - How Membership is managed and how Members are removed
  - Clarify which parts of a CWG charter is allowed to deviate from the Bylaws
- ~~Ambiguity for where to send/post CWG meetings~~
  - ~~We should clarify that CWG meeting minutes must be sent to the CWG public list AND the public web site~~
- ~~All Forum/CWG elections should be handled at the Forum level~~
  - ~~Need consistency, practicality for the election and voting procedure of new officers~~
- ~~Update "Associate Member" categories in Bylaws/Charters:~~
  - ~~Certificate Issuer (probational state)~~
  - ~~WebTrust/ETSI/ACAB-c/FPKI (more "permanent" state)~~
  - ~~Perhaps call it "Probational Certificate Issuer" category (open to other category name ideas)~~
    - ~~1 year duration, renewable~~
    - ~~Explicitly call out privileges (e.g. attend teleconferences and F2F meetings, post to mailing lists, access to wiki, private mailing list)~~

Issues with Bylaws - Charters

- ~~Consolidate Root Certificate Issuer and Certificate Issuer~~
  - ~~They are effectively the same~~
  - ~~Same Membership requirements, no different treatment in the Bylaws/Charters~~
  - ~~Maintaining two titles only creates administrative overhead~~
- ~~Resolve the "third-party" website requirement for SCWG Charter~~
  - ~~Either justify the need to be a "third-party" site for SCWG or remove~~
  - ~~If the decision is to keep, possibly extend to other CWG Charters (Code Signing, S/MIME)~~
- ~~Remove the need to "READ" the antitrust statement before each meeting~~
  - ~~Most promising proposal is to incorporate the antitrust statement by reference, along with the Code of Conduct and IPR policy, as handled at other standards bodies~~
  - ~~Each meeting could begin with: *"All participants are reminded that they must comply with the CA/Browser Forum anti-trust policy, code of conduct, and intellectual property rights agreement. Please contact the chair with any comments or concerns about these policies".*~~

Issues with Bylaws - Charters

- ~~Check for consistency of provisions between Forum Meetings and Forum Teleconference~~
  - ~~Forum Meetings were supposed to be the F2F meetings~~
  - ~~Forum Teleconferences were supposed to be the remote teleconferences~~

Tasks for Infrastructure SC

- Minutes
  - Currently all CWG/Forum-level meeting minutes are listed in a single page
  - Suggest using “tags” that can help separation. The most obvious tags are “CWG name”, “Forum”, but we could also add whether these are for a “teleconference” or a “F2F meeting”
- Workflows for new ballots via member tools and/or GitHub issue forms and pull requests
- Allow only CABF Members to contribute to GitHub (issues or PRs)
  - Create a disclaimer that one must be a CABF Member otherwise issue will be closed and comment ignored
  - If we manage to limit access-control, if a CABF Member wants to contribute, send their GitHub account to the Infrastructure SC (or WG Chair/Vice-Chair) and permissions will be granted

Define specific release cycles for Guidelines

- Current issues
  - Administrative burden for officers (SCWG had 7 ballots updating Guidelines since 1/2023)
  - CAs may need to implement changes outside their regular development cycles
  - Auditors are often not prepared or **do not have defined audit criteria** to assess new requirements
  - Alignment with other SDOs (ETSI/WebTrust) is very challenging
  - Auditors are confused and have no uniform guidance for resolving conflicts caused by different versions of CABF/ETSI/WT during an audit period
- Proposal (*updates to the Bylaws are required*):
  - Ballots and IP Review continues as-is
  - **New Guidelines** incorporating Ballots with cleared IPR to be released twice a year (**March 15, September 15**). Allow CWGs to pick different release dates?
  - **Emergency Guidelines would be released bypassing the 6-month default**. Decision about whether a Ballot is declared an "Emergency Maintenance Guideline", with proper justification, could be done **by consensus of the CWG Voting Members** or if there is **no Consensus via a separate Ballot** with a strict 7 days discussion and 7 days voting period

Control Matrix for Guidelines (future)

- ~~Multiple Baseline Requirements~~
- ~~Overlapping requirements~~
- ~~Most requirements meaningfully the same and just replace e.g. TLS with S/MIME or CodeSigning~~
- ~~Add requirement identifiers and be able to extract these in a spreadsheet~~
- ~~This assists CAs and auditors which will have a clean checklist of requirements that need to be followed and what controls mitigate/satisfy each requirement~~
- ~~This is **especially useful** for CAs that issue **multiple certificate types** and try to align operations and controls~~

Open items (Forum-level)

- Charters alignment (Dimitris + Paul)
- Guidelines specific release cycles (Dimitris)
  - twice a year except for emergencies
  - Ballots will still pass but the effective date will be upon the release of the next Maintenance Guideline
- Bylaws update to introduce an additional option (e-voting) for CA/B Forum Officers (Dimitris)
  - Requires Administrative overhead to initiate the vote compared with initiating the vote via email
  - Convenience but additional learning curve
  - Anonymity of the votes
- BR of BRs (Paul)
  - IPR challenges
  - All WGs must first commit that they will do efforts to align with the BRoBR, override only in a justified and documented way and avoid duplication.
  - Numbering scheme (use RFC 3647 outline but extend and lock down the numbers). Try not to overlap sections in different Guidelines.
- Conflicting sections updated by two or more ballots at the same time (issue #42)
- Make Recordings available?
  - Make Teleconference and F2F Meeting Recordings available via the Member Mailing Lists until minutes are approved
  - Recordings are confidential and must not be distributed outside the Members. Obligation to delete local copies after minutes are approved. Do we need to add to the Bylaws?

Open items (Forum-level) (continue)

- Delegated Third Parties (Dimitris + Paul) to raise awareness to CWGs
  - Each WG must clarify independently but this may be duplication of work, especially in the risk-assessment
  - Possible **alternative audit schemes for DTPs** (ISO/IEC 27001, SOC 2, IASE 3000, ENISA 715, FedRAMP Moderate, C5:2020, CSA STAR CCM, or equivalent, independently audited and certified or reported).
- Misunderstandings that lead to multiple incidents must trigger a review process in the affected guidelines (Paul)
  - Ask Browsers to report for repeated incidents and language from the Guidelines that contributed to the incidents. Possibly creating issues with a certain tag “repeated-incidents”
- IPR Review for a **Maintenance Guideline** to **10 days by default**, unless a Member needs more time, in which case it will extend to 30 days without any other procedure. (Dimitris)