I wanted to capture some of the discussion on the Governance Review WG call today. Maybe we group edit it, and provide to the Forum members for comment? I have tried to make this as neutral and fair as possible.

Problems being addressed

- CAs and one browser participant worked on code signing guidelines in a Working Group, but the guidelines were defeated in a ballot at the Forum level by the vote of two browsers. The two browsers questioned whether code signing was within the scope of the Forum's mission (especially if the result is a set of guidelines followed by only one vendor), and also may have wanted the ballot to fail so the IPR disclosure requirements would not apply and they would not have to disclose their IPR or face RAND-Z free licensing
- The scope of the Forum is arguably too narrow to allow non-SSL certificate working groups and ballots. Bylaw 1.1 provides:

  1.1 Purpose of the Forum:

  > The Certification Authority Browser Forum (CA/Browser Forum) is a voluntary gathering of leading certification authorities (CAs) and vendors of Internet browser software and other applications.
  >
  > Members of the CA/Browser Forum have worked closely together in defining the guidelines and means of implementation for best practices as a way of providing a heightened security for Internet transactions and creating a more intuitive method of displaying secure sites to Internet users.

  In addition, the two browsers who voted against the code signing guidelines ballot may have been concerned that the working group was two narrow (with only one code signing user participating at the working group level)

- "Interested Parties" are allowed to fully participate today on Working Groups under Bylaw 3.2, but must first sign the Forum's RAND-Z IPR agreement. Two code signing certificate users, Adobe and Oracle, declined to participate in the working group, perhaps because they didn't want to sign the IPR agreement (this should be confirmed).
- CAs would like the Forum (in some form) to be able to work on non-SSL issues such as code signing, S/MIME, and client certificate usages, in large part out of convenience (many of the main CA players are already involved in the Fourm, and it is convenient to schedule calls and meetings in the current structure). Some CAs have suggested simply creating spin-off, parallel new groups to handle non-SSL cert issues (using Forum Bylaws and other procedures where relevant), but others would prefer not to set up parallel groups for these other certificate uses, but instead keep in inside the Forum in some manner.
- Some members may want to move from the current RAND-Z IPR covering all Forum and working group activities as a whole, while others may be interested in a W3C-type "participation" model, where the RAND-Z IPR requirements only apply to those Forum and Working Group members who

actually participate on an issue or guideline. Adding procedures to track "participation" for IPR purposes adds complexity, but W3C has rules that could be used as a model.

There are at least three basic options for moving forward. (Ballot 165, which was adopted at the end of March and set up the charter for the Governance Review Working Group, is included at the end of this message.)

Option 1 – Make No Major Changes / Keep Forum Focused on SSL Only

Under Option 1, make no major changes to Bylaw 1.1 – Purpose of the Forum and do not change the current IPR Agreement, membership rules, voting rules, etc. Eliminate any working groups dealing with non-SSL certificate issues (e.g., code signing working group)

Pros: Keeps Forum focused on its main business – SSL certificates. If new separate groups form for code signing, etc. (perhaps using Forum Bylaws and procedures as a starting point), helps those groups focus on their business and avoids cross-group problems with IPR policies, voting rights, etc.

Gives new groups (e.g., code signing, or "Non-TLS Certificate Forum") freedom to adopt different IPR policy, voting rules, etc. Can set separate times and places for meetings (avoid time conflicts with Forum meetings)

Allows non-CA, non-browser members of new groups to participate on an equal basis with CAs. Avoids "dilution" of control, participation from current limitation of CAs and browsers (with "skin in the game")

Cons: Loss of efficiency, harder logistics for CAs already interested in both SSL and non-SSL certificate issues. Potentially more overhead (separate websites, email systems, etc.)

Open Questions: If new groups are created (e.g., code signing group), will application users like Adobe and Oracle participate? If not, probably won't be successful. Will users like Adobe and Oracle sign a RAND-Z IPR agreement (as they would be full participants for each new subject matter organization they join)? If not, how to deal with IPR issues.

Option 2 – Keep Forum as parent focused on SSL, allow non-SSL WGs to be independent

- Under this option, SSL certificate issues would remain at the Forum (parent organization) level, with no change in IPR policy or voting rules
- The Bylaws would be amended to allow non-SSL cert issues to be worked on at the WG level
- The IPR would be amended to limit reach of the IPR disclosure and licensing requirements based on "participation" level but would remain a RAND-Z (royalty free) basis. CAs and browsers would be bound by the IPR agreement on SSL cert issues as they are today, but not on the work of non-SSL cert WGs. Non-SSL WGs would have authority to approve and enact ballots at the WG level, and would not forward them to the Forum for approval or a new ballot (and so avoid triggering IP disclosure requirements at the Forum level). In this way, non-SSL cert WGs can be autonomous, and participants in the WGs will be protected by a RAND-Z IPR, but NON-participants of a particular non-SSL WG would NOT have to disclose any relevant IPR on a WG proposal.

- The Forum would charter all new WGs (both SSL-cert related WGs, and non-SSL cert related WGs), and would set the voting rules for non-SSL cert WGs (e.g., final WG guidelines must be approved by 2/3 of WG members, as there will not be separate classes of CAs and browsers in these non-SSL cert WGs. We may need to set voting limits for participants who don't have "skin in the game" so the non-SSL cert WGs can't be taken over by individual participants who are not CAs or applications).

Pros: Allows the Forum to work on non-SSL cert issues at the WG level, without forcing Members only interested in SSL to participate or vote on non-SSL guidelines and have to disclose or license their IP if a guideline passes (and without forcing those Members to veto a proposal for this reason). Maximizes efficiency for those CAs who want to work on both SSL cert and non-SSL cert issued in the same Forum and at the same meetings. Avoids duplication of overhead (web page, mailing lists, meetings, etc.) when working on non-SSL cert issues. Interested Parties can already participate in WGs if they sign the IPR, so no change is required there.

Cons: Non-CAs/non-browsers who are participants in WGs could feel like second class participants because they don't have a vote at the Forum level on formation or charter of WGs, voting rules, etc. (but this is the case today for Interested Parties, plus CAs who are Forum members would probably represent the interests of those participants at the Forum level anyway). Option 2 will be more complex than what we have today. Moving to a "participant / RAND-Z" IPR system will require more record keeping as to who is or was a participant (like W3C), so is more complex (but, so long as we limit a duty to disclose to those who sign up for a particular WG, and maintain our standard RAND-Z IPR agreement for each WG, it may not be that complex).

Open Issues. Will applications like Oracle and Java agree to join a WG if they have to sign our current RAND-Z IPR agreement (even if disclosure is limited only to those issues in those WGs in which they participate)? Unknown – need to ask.

Would this Option 2 satisfy the browsers who voted no on the code signing guidelines at the Forum level? Unknown – need to ask.

Option 3 – Restructure Forum to Be Management Only, Put SSL Cert and other Issues in Separate WGs

- Under this option, Bylaws would be amended so the scope of the Forum covers all types of certificates and all work of the Forum would be done at the WG level, and the Forum itself (parent level) would just perform a management and coordination function, but not work on substantive issues or vote to adopt particular guidelines. It is likely that "members" at the Forum level would be more like an executive committee made up of representatives of the various WGs – SSL certs, code signing certs, S/MIME, client certs, etc. – so the Executive Committee membership would no longer be just CAs and browsers. The Executive Committee would set meeting dates, charter new WGs, set participation requirements (e.g., "skin in the game"), set a uniform IPR policy for each WG, maintain participation records and copies of guidelines adopted at the WG level, etc. The name of the Forum might need to be changed to reflect the broader reach of all the WGs, such as "PKI Forum" (already used elsewhere).

- Modify the current IPR agreement to be “participation only” based on WG participation – but continue to be RAND-Z. The IPR agreement would probably be uniform for each WG, probably adopted at the Forum Executive Committee level.
- Guidelines would be developed and adopted at the WG level, according to voting rules set by the Forum (for the SSL cert WG, it might be the same voting and participation rules we have today; for other WGs, there could be a simple rule such as approval by 2/3 of all WG members, perhaps with voting sublimits applied to participants who are not involved in the commercial work of the WG subject – e.g., are not a CA or a relevant application). Guidelines adopted at the WG level would not be reviewed or approved at the Forum Executive Committee level, so no IPR agreement requirements would ever occur at the Forum Executive Committee level

Pros: This creates a certain symmetry – all WGs are equal and fairly independent, with SSL certs being treated no differently from code signing certs, etc. We could leverage the experience of the current Forum in running these types of WGs, and would enjoy the efficiency of having the various WG meetings occurring at the same location during the same week (which would allow CAs to participate in all the WG meetings if they have an interest). When the work of WGs overlaps, the Forum Executive Committee would coordinate and avoid conflicts. Using a standard, participation-based RAND-Z IPR agreement at each WG level would avoid confusion. Browsers would need only participate in the SSL certificate WG if they want, and not be exposed to any of the other certificate issues or IP disclosure and licensing requirements.

Cons: The Forum has 11 successful years behind it in raising the bar for SSL certificates, and risks losing that track record and diluting its effectiveness if SSL certificates become only one WG of many. It’s not clear that very many new participants will show up and participate in the non-SSL cert WGs compared to today (or will sign a participation based RAND-Z IPR policy), so why make all these changes if it doesn’t increase participation? If some WGs want to go to a non-RAND-Z IPR agreement form, will the Forum allow this, or will the Forum say no?

By converting the Forum level from an SSL certificate group to an Executive Committee coordinating group (with non-CAs and non-Browsers represented), CAs and browsers will lose power in setting the direction for the Forum and its WGs, and ultimately the Forum Executive Committee could do things that CAs and browsers don’t like – e.g., drop IPR agreements for all WGs, limit the scope of the SSL certificate WG, etc. – why take that risk?

If participation in various WGs grows, will the WGs be able to meet in the same location during the same 3-day period as our current Forum meetings? Or will some WGs want all-day meetings to work on more ambitious projects? If the latter, we may lose some of the efficiency of this approach, and might as well ask the WG to leave the Forum and just become its own new organization.

Open Issues: Will applications like Oracle and Java agree to join a WG if they have to sign our current RAND-Z IPR agreement (even if disclosure is limited only to those issues in those WGs in which they participate)? Unknown – need to ask.

Would this Option 3 satisfy the browsers who voted no on the code signing guidelines at the Forum level? Unknown – need to ask.

Would this Option 3 require more administrative duties at the Forum Executive Committee level than we are equipped to provide as a volunteer organization with no funding or staff? Hard to say, but could be a challenge if the number of WGs and numbers of participants on each WG grows too large. We can't be a copy of W3C with our current resources.

*****

B**allot 165 - Formation of Governance Review Working Group**
The following motion has been proposed by Dean Coclin of Symantec and endorsed by Robin Alden of Comodo and Kirk Hall of Trend Micro:
-- MOTION BEGINS --
In accordance with Section 5.3 of the CA/B Forum Bylaws, the chartering of a new working group by ballot is required. This Ballot proposes chartering of the Governance Review Working Group. The Working Group's charter will be as follows:
1. Consider revisions to the scope of the Forum to include possible additional topics such as code signing, SMIME and client certificate usages
2. Review the scope of the IPR and IP ownership issues
3. Consider options for representation of others in forum issues
4. Review voting rules and rights
5. Review admin functions
6. Examine making the forum an "official" organization (e.g. Incorporation)
7. Review how requirements and guideline documents would be structured in a newly organized forum would be done
The group's deliverables will be:
1. An extensive report with one or more proposals on possible changes to the Forum organization ("proposed structure")
2. A proposal on requirements and guideline document structure and proprietorship
3. A form of ballot or ballots to implement any recommendations
The Working Group shall expire once the deliverables have been completed.
-- MOTION ENDS --
The review period for this ballot shall commence at 2200 UTC on 17 March 2016, and will close at 2200 UTC on 24 March 2016. Unless the motion is withdrawn during the review period, the voting period will start immediately thereafter and will close at 2200 UTC on 31 March 2016. Votes must be cast by posting an on-list reply to this thread.
A vote in favor of the motion must indicate a clear 'yes' in the response. A vote against must indicate a clear 'no' in the response. A vote to abstain must indicate a clear 'abstain' in the response. Unclear responses will not be counted. The latest vote received from any representative of a voting member before the close of the voting period will be counted. Voting members are listed
here: https://cabforum.org/members/