# Server Certificate Working Group

Discussion Leader: Inigo Barreira (Sectigo)

Minutes: Tim Callan

Presentation link:

Discussion outside the presentation:

## Summary

Inigo read the anti-trust statement.

## Agenda

Agenda reviewed and approved.

## Minutes

May 9 minutes were distributed May 13.

Inigo asked for comments and received none.  Minutes approved.

## Membership applications

Two new applications for membership:

\* One interested party Aryan in a personal capacity.  Inigo sees no issue adding to this WG. There are no concerns and Aryan is added.

\* Full membership application by Brainit.sk. This company is listed in the UTL but it does not appear to be in the root stores. This company has not provided test certificates.

- Inigo does not believe they can be full members.

- Dean concurs.

- Dean to reply and say they don't meet the current requirements.

## Summary

Summary of this quarter:

\* We had many ballots this quarter. 6 ballots:

\* SC73, SC72, SC65, SC69, SC70, SC68

\* SC73 is under IPR review and will probably finish next week or the week after.

\* SC74 (CPS clarification) failed.

Under discussion: SC67 (MPIC), SC71 (subscriber agreement)

Under consideration: two ballots

New TLS BR versions:

\* 2.0.3

\* 2.0.4

\* 2.0.5 should SC73 go into effect.

3 EVG versions.

New PAG SC to deal with GoDaddy IPR claim.

Number of open issues  in GitHub were reduced but recent discssions have made them grow

We have a new triage process.

Inigo asked for feedback.  Ben said he likes it.

Many email threads on the distro list.

Validation SC summary:

\* Corey will provide better review tomorrowl

\* MPIC

\* Automation

\* DTPs

Achievements and goals:

\* Slot update

\* New charter

\* Many ballots

\* New EVGs format

\* Change WG teleconferences content

Goals

\* Goals are listed in the presentation

## Presentations/Topics

### PKI Metal

Making Linting Easier. Talk by Rob Stradling of Sectigo.

SC 75 is considering requiring linting and Chrome has stated it's a very important priroity.

Implementing linters is actually a hard engineering challenge.

An entire raft of issuance bugs could have been avoided if we used linters available.

We would like to make no excuse for any CA to lack preissuance linting

Rob's experience:

\* crt.sh

\* Linting newly issued certs is too slow

\* Updating linters is awkward

\* Need to add support for pklint

\* Sectigo's CA

\* Need to future-proof performance

\* Updating linters is a bit awkward

\* Ongoing code modernization

Ecosystem observations

\* SC75 is codifying existing understanding of linters' value

\* Using multiple linters is a best practice

\* There are also special purpose linters that do one thing well (will mention examples later)

Integrating linters into a CA system is awkward

\* They are in different programming languages

\* Implementing as preissuance linters can be difficult

\* Many are written as command line functions.  In some cases it can take half a second to issue just one certificate.

\* Many of the CA action items in Bugzilla are integration of Linters, that are often a far time away.

Many CAs are tackling and struggling with the same set of linter integrations

\* Pain points

\* Integration

\* Upgrading

\* Performance

Introducing PKI Metal

\* Provides access to multiple linters via a single API call

\* Supports pre certs, certs, OCSP as input, and CRL

\* Auto detects the intended profile

\* Combines the results of all the linters into a single response

\* Supports preissuance and post issuance linting

\* Can run multiple instances of every linter

\* You can disable any linter you dn't want to use

\* A modular design to make integration of new linters easier in the future

\* Dockerized

Supported linters

\* certlint

\* x.509lint

\* zlint

\* pkilint

\* dwklint (weak keys according to SC73)

\* FTFY

Will be opened soon in GitHub

Would like to encourage it to be a community project and not just a Sectigo project.

Please reach out to rob@sectigo.com with questions, feature requests, etc.

Questions:

\* Each CA will operate its own instance if able to and otherwise can use the public instance we are making available.

\* It can be used total on prem.

\* Mads: Will the rate limits on crt.sh change?

\* Rob is planning on making it backwards compatible.

\* When he updates it, will it change anything? Rate limits make the lint service unavailable.

\* Rob says the reasons for those rate limits will go away,  Should take a higher rate.

\* Nicol: Updating underlying linters is a problem because it triggers QA.  So how would that work with PKI Metal? Do we update PKI MEtal itself or the underlying linters or what?

\* Rob: If you're using it dockerized, you'll just update PKI metal and it will contain each of the linters.

\* Ryan: This is incredible and this looks valauble to the community . I can't wait to try this out. Thank you.

\* Paul: I suppose you use GitHub actions. Have you thought about incorporating a test corpus before new releases? When people in the ecosystem start relying on PKI Metal, there is an expected quality. They may adopt the new versions without testing it themselves.

\* Rob:  Agreed.  Quality will be important.

\* Dimitris: As the discussion for SC75 is progressing, the expectation was that each CA would have to add controls for linting. It will be their responsibility.

This may be an opportunity for the linting ballot to add language about updating.  Blindly applying new linters is not necessarily a good choice.

How do you plan on handling updates?

\* Rob: This body should think about that policy.

\* Rob asks if any CAs have linting completely under control and have no interest in this.  Nobody says yes.

\*Dimitris: KeyFactor had a similar proposal.

\* Rob: It's possible to have multiple solutions for a problem.

### SwissSign - Organization Identifier

Adrian Mueller and Sandy Balzer

Setting some fields to optional if set

About EV naming fields: CABForganizationIdentifier

They suggest to make the CABFOrganizationIdentifier optional

cabfOrganizationIdentifier is a SHALL for OV and Sponsored S/MIME. It's a MUST in EV. Not required in ETSI

Suggesting of OrganizationIdentifier is included, JoI and SerialNumber can be optional.

Benefits:

\* Reduced complexity

\* Clear requirements

\* Less error prone

Tim Hollebeek:

\* Making the CABF OrganizationIdentifier optional would be fine

\* Every like the organization identifier.

\* The other I have to think about.   Your argument makes sense.

\* As the organization identifier is not mandatory,  you would make finding a serial number in a certificate in an automated way more difficult.

Dimistris: TLS implementations have a challenge because some browsers will display the information from the JOI. But it makes sense to remove the redundancy. I would love if certificate consumers could use that information.

Clint:

I don't want to get rid of the CABF OrganizationIdentifier

Tim H: The way this happened was PSD 2.  If that's your position, we're stuck with both until the end of time.

[Break]

### Client Authentication

Dimitris: On Bugzilla a CA issued a client cert from a TLS-capable issuing CA. It had a client EKU but not a TLS EKU. I looked at the TLS BRs to figure out if this is in scope or not.

Before SC62, issuing a client auth cert was allowed. After it was not.

I was looking for clarity if this was the intended effect.

Clint is of the opinion it is on purpose.

If there are no objections or counterarguments, it would be helpful to add to the BRs.

Paul: I think it would have been a long term goal. We did highlight the changes with the introduction of the ballot. If it was an intended change, why did we not include it in the change list.

Clint: I think it is included in the change list to the extent that the TLS BRs can include it. The scope of the BRs doesn't cover the leaf certificates issued by the CA but does cover the CA itself. It wasn't made as explicitly clear as Dimitris stated it.

Dimitris: As one of the endorsers of SC62, I would remember if it was something so intentional. But if there is agreement that this is the way we want to go, I'll either create an issue to put it in a clarificatino ballot to clearly state that TLS issuing CAs should only issue TLS certificates.

### Legal name and DBAs

Martijn Katerbarg:

This comes out of an issue we had recently where we had LEGAL NAME dba TRADE NAME. I have a proposal.

Current allowed practice:

\* EV  legal name or dba (legal name)

\* OV is one or the other.

Propose expanding OV to at least allow the current example allowed for EV. Also allow DBA inclusion with both names

Martijn proposed DBA, D/B/A and local equivalents.

Case-insensitive approach.

And do we want to add the fourth option to EV also?

Paul:

\* Is DBA going to confuse people as an abbreviation?

\* Couldn't we use Subject Alternative Name for that?

Scott Rea:

\* I think there is a difference in what is displayed by the clients?

Paul:

\* Are users actually going to understand this?

Martijn:

\* Are users understanding the EV example either?

\* That's why I included the local reference.

\* Adding to Subject Alt Name is additional things for CAs to take care of, and it seems like an additional complications.

Paul:

\* We could think about another subject attribute.

### SCWG Document Publication Procedure

Inigo Barreira:

There have been significant changes in SCWG. Many ballots and versions of BRs and EVGs. In New Delhi, we talked about a new way to publish versions of the BRs and EVGs. At one point we were running 3 ballots at a time.  Changing from one to another was difficult.

Proposal:

\* 2 types of ballots.  Regular ones and emergencies.

\* New version publication:

\* Approved ballots are merged into the guideline for publication at the end of the quarter.

\* Will include all descriptions.

\* Adopted date will be date of publication

\* Effective dates TBD

\* Emergency ballots:

\* Same procedure as now.  Publish its own version.

\* Potential issues:

\* Different branches affecting the same section

\* Emergency ballot conflicts with a passed ballot awaiting publication

Tim H:

\* Would be first on month, not 15th.

Dimitris:

\* This similar to what we discused in the past. I proposed twice a year.

\* We need to change the by-laws.

\* I believe it makes sense.

Clint:

\* I'm reticent to embed effective dates into bylaws and charters.

\* It's gone a lot better to have the general consensus to to focus on specific dates.

\* If gives us flexibility we would lose if the introduce it into the bylaws.

\* My concern is that if we do it wrong, effective dates can be lost six months. We have lost that period where there is a requirement in a document but it's a future effective date.

\* I feel like in practice this could be used as an excuse errors.

\* Maybe drafting language would help us with how we would address those.

\* We can work on language.

### GitHub open issues

\* We looked at issue #272 Martijn: Is this just a cleanup ballot thing?

\* #273. Formatting error.  Put in cleanup.

\* #274. Clarify if 3.2.2.8 can be delegated.

\* #278/279 Clarify behavior when an effective date predates its own publication date.

\* #303 Remove reference to code signing and focus language on TLS.

\* Inigo:  Do we have any such language?

\* #306 Clarify OCSP profile

\* Clint:  I think this was fixed in SC62.

\* Ben: I think this issue is it was in the wrong section, and I'm not sure we put it in the right section.

\* Clint: It's in 1.7.2.8.  So the profile piece at least was fixed.

### Ballots

We have ongoing ballots under discussion period:  MPIC and linting.

Ryan, can you give a summary of where we are?

Ryan: We received limited discussion in round 2.  We incorporated small changes.  No discussion for round 3.  We intend to commence voting on Monday.

Dimitris: If a CA wanted to try to test MPIC, are you aware of any implementations that a CA could use today to test it.  I know there are open APIs from Cloudflare and maybe others.

Ryan:  We have no feedback on any CAs who have tested. In the ballot preamble we included a link to the Princeton team to accomplish the same goal. We have had no feedback from Princeton or Cloudflare on adoption.

Prelinting ballot.

Dimitris:

\* The discussion is going well. There is discussion of phasing it in.  September 2024 would be a SHOULD and March 2025 would be a SHALL.

\* There is a question about if we will add updating language.

### Other business

Scott Rea:

\* I asked a question on the list but I didn't get all my answers.

\* This is around when we do voting.

\* There is a requirement about quorum and measuring that.

\* Some aspects weren't clarified.

\* Section 6 of the charter defines quorum but doesn't say you need quorum for a valid vote

\* Does this need to be clarified.

\* There is a thing about being in the previous 3 meetings.  Is this from the start of the ballot or the end of the ballot or what?  This needs to be clarifieid.

\* We need to have at least 1 from each category.  Is that sufficient?  Do we need more than that?

\* At least at SCWG this should not be an issue.

Dimitris: Quorum is required in the bylaws for voting.  The charter is trying to align with the bylaws.

Scott: I agree that's implied, but the charter is allowed to deviate.  So we should make it explicit.

There was a question about if the bylaws say it or not.

Scott: The real issue is how to we measure when it starts.

Dimitris: This is answered in the bylaws also.  It's the last 3 meetings after the voting period stops.

Scott: How about only requiring one and not more than one from each category in SCWG.

Wayne: The real reason for that requirement is to CAs can't pass something without at least one browser consenting.