Technical Advisory Council (TAC) Meeting

October 6, 2022

CONFIDENTIAL COMPUTING CONSORTIUM

This meeting is being recorded.

The Confidential Computing Consortium

A community focused on open source licensed projects securing DATA IN USE & accelerating the adoption of confidential computing through open collaboration

Every member is welcome; every project meeting our criteria is welcome.
We are a transparent, collaborative community.

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

CONFIDENTIAL COMPUTING CONSORTIUM

Antitrust Policy Notice

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.
- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

CONFIDENTIAL COMPUTING CONSORTIUM

Roll Call, and Introductions of new attendees

Quorum requires **5** or more voting reps:

Member	**Representative / Alternate**	**Email**
Accenture	Giuseppe Giordano	giuseppe.giordano@accenture.com
Ant Group	Hongliang Tian (Tate)	tate.thl@antgroup.com
Arm	Thomas Fossati / Michael	thomas.fossati@arm.com
Facebook	Eric Northup / Shankaran	digitaleric@fb.com
Google	Cfir Cohen / Catalin Sandu	cfir@google.com
Huawei	Zhipeng (Howard) Huang	huangzhipeng@huawei.com
Intel	Dan Middleton / Simon	dan.middleton@intel.com
Microsoft	Dave Thaler(*)	dthaler@microsoft.com
Red Hat/IBM	Lily Sturmann / Dimitrios	lsturman@redhat.com

** TAC chair*

CONFIDENTIAL COMPUTING CONSORTIUM

Etherpad - Meeting Minutes

- https://markdown.etherpad.com/p/CCC-TAC-Minutes-2022-10-06

- Join the etherpad and set up your name and text color
  - Meeting attendance - please **add yourself**
  - **Voting Attendees just need to put a “+” next to their name**

- **Please** help make the meeting minutes be more accurate

- Export document in Markdown (GitHub docs), PDF

CONFIDENTIAL COMPUTING CONSORTIUM

Agenda

1. Welcome, roll call, introduce any first-time attendees
2. Approval of minutes
3. Action item review
4. Tac Tech Talks:
    - RISC-V Trusted Computing WG
5. IETF Hackathon
6. Common Test Infrastructure
7. Outreach committee
    - CCC Landscape and Solutions Map - Nick Vidal
    - New Website, status
8. Common Terminology whitepaper working session
9. Election timeline
10. Review of open pull requests/issues (time permitting)
11. Any other business

CONFIDENTIAL COMPUTING CONSORTIUM

Approval of TAC Minutes

https://github.com/confidential-computing/governance/pull/138

Proposed:
That the minutes of the September 22, 2022 meeting of the Technical Advisory Council meeting of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

CONFIDENTIAL COMPUTING CONSORTIUM

Action Item Review

1. [Mentors] Mentors to reach out to the project for getting the maintainers involved in Common Test Infrastructure (Gramine not interested)
2. [Kurt] to set up a meeting to define scope and technical requirements for Test Infrastructure with LF IT, Dave T, Dan M, Alec F, Nick V (LF IT ready, need to determine if the projects still want to move forward)
3. [Kurt] determine if the 100K “Consortium IT Services and Collab Tools” budget item is available to move to funding travel for select conference attendees (Added to agenda, confirm at Oct 19th Governing Board meeting)
4. [Kurt] to provide approved language for new projects process intake form (PR created - https://github.com/confidential-computing/governance/pull/139)

TAC Tech Talks

- RISC-V Trusted Computing WG - Suresh Sugumar

IETF Hackathon

https://www.ietf.org/how/runningcode/hackathons/115-hackathon/

- Thomas Fossati:
  - We were thinking of having a “CC table” at the IETF hackathon [1] in London [2] (5-6 Nov), and do some CCC advocacy there. … From the Arm side we could bring a bunch of OSS technology that’s in scope with both CCC and IETF (Veraison, mbedTLS, PARSEC) and use it as a gateway for evangelising and further cross-pollination (e.g., with TLS, TEEP, and obviously RATS).
- Budget request from Veraison project:
  - “In discussion with the Veraison team that is planning to attend, they are looking for about $1K to cover the cost of their travels to the event. This is a weekend event and 2 of the 4 volunteers are local, hence the minimal cost to attend.”
- Outreach committee: not about sponsoring event, so this is a TAC question
  - Stephen Walli: “There is lots of money in the TAC, Outreach, and budget surplus. The answer should be, yes.”
-

PROPOSED:

Projects can request up to $2k per year for travel to hackathons or conferences for open source projects to promote and/or test their project

Requests are approved by the TAC on a case by case basis

Common Test Infrastructure

- **Discussion: still desired?**
  - **Feedback so far is that it might not be used this year**
- **Needing**:
  - LF IT ready to meet for sizing and technical requirements
  - Available CCC leads time to meet - resend email?
- Approved: 50K for infrastructure management and 15K for hardware
- Would any project use such infrastructure if it existed?
  - Projects: Enarx yes, OE no, Gramine no, Occlum ??

Updates from Outreach Committee

- Landscape and solutions map
- Wikipedia Confidential Computing Consortium page
  - Outreach will use the first whitepaper as a template and TAC will
  - Currently redirects to LF page
  - https://en.wikipedia.org/w/index.php?title=Confidential_Computing_Consortium&redirect=no
  - Alternate effort also do a confidential computing page
- https://en.wikipedia.org/wiki/Trusted_execution_environment
- New Website, status

CONFIDENTIAL COMPUTING CONSORTIUM

Establishing common terminology - Whitepaper

Doc in progress:

- https://github.com/confidential-computing/governance/blob/main/terminology/common-terminology.md
- LF Creative Services engaged for document conversion and formatting for whitepaper PDF, needs to be finalized for last updates to LF CS
- PR's:
  - https://github.com/confidential-computing/governance/pull/132
- Issues:
  - https://github.com/confidential-computing/governance/issues/123

CONFIDENTIAL COMPUTING CONSORTIUM

Election timeline

- FRI Nov 4, 2022 (Nov 6, **2019)**: Call for nominations opens
- THU Nov 10, 2022 (Nov 12, **2020** / Nov 10, **2021)**: Call for nominations closes
- WED Nov 16, 2022 (Nov 18, **2020)**: Voting period opens
- WED Nov 23, 2022 (Nov 25, **2020)**: Voting period closes
- TUE Nov 29, 2022 (Dec 1, **2020** / Nov 30, **2021)**: Election results announced

CONFIDENTIAL COMPUTING CONSORTIUM

Time permitting: Review of open issues and PRs

Current open issues in the Governance repo:
https://github.com/confidential-computing/governance/issues

Current open PRs in the Governance repo:
https://github.com/confidential-computing/governance/pulls

CONFIDENTIAL COMPUTING CONSORTIUM

Any other business / Schedule

Date	CCC Project Review	TAC Tech Talk
22 SEPT 2022		NSF Center for Distributed Confidential Computing (30 min) - Prof Xiaofeng Wang MPC + TEE (30 min) - Jordan Brandt
6 OCT 2022		RISC-V Trusted Computing group
20 OCT 2022		
3 Nov 2022		
17 Nov 2022		

Tentative TAC talk topics

- Rust Hypervisor firmware: https://github.com/cloud-hypervisor/rust-hypervisor-firmware - Dan to provide contact
- Trust domains - Mike?
- Defined-Trust Transport (DeftT) Protocol for Limited Domains - Kathleen Nichols, Van Jacobson, Randy King
-

CONFIDENTIAL COMPUTING CONSORTIUM

Budget as of 7/31/2022

Description	2022 Approved Budget	YTD Actuals thru July 22	July 2022	Remainder	Notes
License Scanning	$12,000	$0	$0	$12,000	
Test infrastructure	$75,000	$0	$0	$75,000	Common $15k, Project $60k
IT Services and Collab Tools	$3,864	$4,991	$758	$3,790	
Non-Capital Equipment		$4,961	$0	-$4,961	Custom Exxact Workstation & Amazon order (Gramine)
Community Support	$0	$8,000	$8,000	-$8,000	Outreachy
Consortium IT Services and Collab Tools	$100,000	$0	$0	$100,000	
Hosting and other costs	$10,000		$0	$10,000	
Internships	$52,000		$0	$52,000	Outreachy
Subtotal	$257,781	$17,952	$8,758	$239,829	

CONFIDENTIAL COMPUTING CONSORTIUM

Deferred topics

Reference: past TAC tech talk topics

- 2021-10-07: Kata containers
- 2021-10-21: Protecting critical infrastructure
- 2021-12-02: RISC-V security overview
- 2022-01-13: Homomorphic Encryption
- 2022-01-27: OP-TEE and Trusted Services
- 2022-02-10: Confidential computing mentorship
- 2022-03-10: Overview of TCG confidential computing
- 2022-04-07: Governance
- 2022-05-05: IETF Trusted Execution Environment Provisioning
- 2022-05-19: Logging and error reporting in confidential computing
- 2022-06-02: Multi-TEE systems: PCI-SIG WG
- 2022-06-30: Blueprints for Enclaves

CONFIDENTIAL COMPUTING CONSORTIUM

Project	Proposed by	TAC Approved	Tech. Charter	IP Assigned	Board Presentation	Board Approved	Annual Review	Mentor	Webinar
Enarx	Red Hat	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	10 MAR 2022	Nick Vidal	JAN 2021
OE SDK	Microsoft	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	24 FEB 2022	Dave Thaler	MAR 2021
Gramine	UNC Chapel Hill	2 APR 2020	Yes	Yes	1 DEC 2021	15 SEP 2021	4 NOV 2021	Eric V	FEB 2022
Keystone	UC Berkeley	23 JUL 2020	Yes	Yes	24 JUN 2021	MAR 2021	13 JAN 2022	Stephen & Lily	JUN 2021
Occlum	Ant Financial	20 AUG 2020	Yes	Yes	10 SEP 2020	15 SEP 2021	2 DEC 2021	Zongmin	MAY 2021
Veracruz	Arm	3 SEP 2020	Yes	Yes	19 NOV 2020	14 APR 2021	18 NOV 2021	Thomas F	APR 2021
CCC-Attestation	TAC	Yes	Yes	N/A	18 MAR 2021	18 MAR 2021	21 APR 2022	Dan & Aeva	21 JUNE 2022
Veraison	Arm	4 FEB 2022	Yes	Yes	16 MAR 2022	18 May 2022		Howard Huang	NOV 2021

Reference: CCC project expectations

CCC projects are expected to:

- Participate actively in CCC activities (webinars, newsletters, events, etc.)
- Notify the TAC and Outreach committees of relevant news
- Participate in an annual review with the TAC
- Inform the TAC when dependencies change so records can be updated
- Maintainers should take the Linux Foundation's free Inclusive Open Source Community Orientation training course
- Transfer trademarks and domain registrations to the Linux Foundation

CONFIDENTIAL COMPUTING CONSORTIUM

Code Scanning from the LF

Recap:

- **Intake Scan:** High level scan with an emphasis on finding all open source licenses present in the codebase, and some third party dependencies. We provide a summary report listing the licenses found, including any copyleft licenses and potential license conflicts. We do NOT examine every match to a potential license, and we do NOT provide a detailed file inventory showing where the license matches occur. In order to do any follow up or recurring scans, a full baseline scan will be necessary first.

- **Baseline Scan:** Full scan, where every license match is examined. A detailed report is provided including a complete file inventory for every license match, and detailed findings for any copyleft license or other potential license issues found. This can potentially take significantly longer than an intake scan, depending on the size of the codebase. The baseline scan results are stored and are available for doing incremental / recurring periodic scans.

Reference: CCC project benefits

CCC projects have access to a number of benefits:

- Up to $7,500 in budget for hardware and software per year.
- Funding for one Outreachy intern.
- TAC mentor assigned to the project.
- Collaboration tools (contact operations@confidentialcomputing.io):
  - Zoom
  - Domain registration and renewals
  - Mailing lists
  - YouTube playlists
- Optional security scanning
- LFX tools (https://lfx.linuxfoundation.org).

CONFIDENTIAL COMPUTING CONSORTIUM