

Technical Advisory Council (TAC) Meeting

November 3, 2022

This meeting is being recorded.



CONFIDENTIAL COMPUTING
CONSORTIUM

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.

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 Updegrave of the firm of Gesmer Updegrave LLP, which provides legal counsel to the Linux Foundation.

Agenda

1. Welcome, roll call, introduce any first-time attendees
2. Approval of minutes
3. Action item review
4. Common Test Infrastructure
5. 2022/2023 budget
6. TAC election - call for nominations
7. Outreach committee update
 - New Website, status
 - Landscape - Ben Fischer
8. Common Terminology whitepaper working session
9. Review of open pull requests/issues (time permitting)
10. Any other business

Roll Call, and Introductions of new attendees

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

<u>Member</u>	<u>Representative / Alternate</u>	<u>Email</u>
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

Etherpad - Meeting Minutes

- <https://markdown.etherpad.com/p/CCC-TAC-Minutes-2022-11-03>
- 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

Approval of TAC Minutes

<https://github.com/confidential-computing/governance/pull/143>

<https://github.com/confidential-computing/governance/pull/145>

Proposed:

That the minutes of the October 6, 2022 and October 20, 2022 meetings 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.

Action Item Review

1. [Zongmin/Dan] Mentors to reach out to the project for getting the maintainers involved in Common Test Infrastructure (Gramine not interested), (Occlum is interested - IT administration or just hardware?)
- ~~2. [Lily] Make sure Keystone is participating in RISC-V [DONE]~~
3. [Kurt] to verify that project messaging services are listed on the new website, something similar to eBPF Foundation projects summary
4. [Kurt] Outreach to make sure that events like this have a home in the new website redesign [DONE]
5. [Kurt] see if LF has best practices documentation for growing a community, if not start a document on a CCC wiki page
6. [Kurt] to create TAC Governance Github repo wiki start page (Done)
7. [Kurt] to get more information on how Hyperledger funds a technical project architect/manager (The title used in Hyperledger was "Community Architect") (Asking about process and cost, pending)
8. [Kurt] find out who suggested CDCC investigators and follow up

Common Test Infrastructure - deferred to 2023?

- **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 ??**

TAC 2022 Budget

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 (\$7,500 ➡ 10k) Gramine \$9192 for 2022
IT Services and Collab Tools	\$3,864	\$4,991	\$758	\$3,790	website, slack, groups,io
Non-Capital Equipment		\$4,961	\$0	-\$4,961	Custom Exxact Workstation & Amazon order (Gramine)
Consortium IT Services and Collab Tools	\$100,000	\$0	\$0	\$100,000	Budget for use by projects
Hosting and other costs	\$10,000		\$0	\$10,000	Used if someone needs a software license or something else simple
Internships	\$52,000		\$0	\$52,000	Outreachy (\$6,500 per qualifying project)
Community Support	\$0	\$8,000	\$8,000	-\$8,000	Outreachy
Subtotal	\$257,781	\$17,952	\$8,758	\$239,829	

TAC 2022 Budget / IETF Hackathon

- TAC vote (now concluded):
 - **PROPOSED (for 2022):**
 - 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
- \$2k could be increased but we only have 1 request (Veraison) for 2022 budget for ~\$1k
 - CCC table at IETF hackathon Nov 5-6
- Governing Board approved of shifting part (\$20k) of the unused \$100K “Consortium IT Services and Collab Tools” 2022 budget item to funding travel for select conference attendees

Areas of CCC Focus

1. Project support, incl. cross-project coordination/communication
2. Cross-org coordination
 - a. Standards orgs: IETF, TCG, **RISC-V**, HomomorphicEncryption.org, ...
 - b. Open-source orgs: CNCF, TrustedFirmware.org, ...
 - c. Government agencies: NIST, BSI, ...
 - d. **Academia: NSF Center for Distributed Confidential Computing, ...**
 - e. **Other technical bodies: MPC Alliance, ...**
3. Additional collateral (whitepaper, terminology, talks)
4. Demos and tech talks in TAC meetings
5. Community development & DCI (diversity, civility, inclusion)

TAC 2023 DRAFT Budget

Description	2022 Approved Budget	2022 September YTD	2023 Draft Budget	Notes	Area
License Scanning	\$12,000	\$0	\$0		Project support
Test infrastructure (capital or non-capital)	\$75,000	\$9922	\$60,000	\$10k/project x 6 projects	Project support
IT Services and Collab Tools	\$3,864	\$6,507	\$8,000	website, slack, groups,io	Project support Community development & DCI
Consortium IT Services and Collab Tools	\$100,000	\$0	\$10,000	Misc. budget for use by projects	Project support
Travel expenses	\$0	\$0	\$80,000	\$10k/project x 8 projects	Project support Cross-org coordination
Software licenses	\$10,000	\$0	\$0		Project support
Outreachy (internships/community support)	\$52,000	\$8,000	\$32,000	Outreachy (\$8k x 4 projects)	Community development & DCI Project support
Community management for projects			\$100,000		Community development & DCI Project support
Subtotal	\$257,781	\$17,952	\$290,000		

Election timeline

- FRI Nov 4, 2022: Call for nominations opens
- THU Nov 10, 2022: Call for nominations closes
- WED Nov 16, 2022: Voting period opens
- WED Nov 23, 2022: Voting period closes
- TUE Nov 29, 2022: Election results announced

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

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:
 - [Update common-terminology.md by MikeCamel · Pull Request #134 · confidential-computing/governance \(github.com\)](#)
- Issues:
 - [Terminology: handling of nesting and packaging granularity smaller than TCB · Issue #136 · confidential-computing/governance \(github.com\)](#)
 - [documentation/architecture.md at main · confidential-containers/documentation \(github.com\)](#)

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

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>

Any other business / Schedule

Date	CCC Project Review	TAC Tech Talk
3 Nov 2022		
17 Nov 2022		Occlum Annual Report?
1 Dec 2022		
15 Dec 2022		

Tentative TAC talk topics

- Rust Hypervisor firmware: <https://github.com/cloud-hypervisor/rust-hypervisor-firmware>
- Trust domains - Mike?
- Defined-Trust Transport (DeftT) Protocol for Limited Domains - Kathleen Nichols, Van Jacobson, Randy King
- <Kurt: check with CDCC investigators?>
- Relationship between eBPF and Confidential Computing?

Budget as of 9/30/2022

Description	2022 Approved Budget	YTD Actuals thru Sept 22	Sept 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	\$6,507	\$758	\$3,790	
Non-Capital Equipment		\$4,961	\$0	-\$4,961	Custom Exxact Workstation & Amazon order (Gramine)
Community Support	\$0	\$80	\$0	\$0	
Consortium IT Services and Collab Tools	\$100,000	\$0	\$0	\$100,000	
Hosting and other costs	\$10,000	\$0	\$0	\$10,000	
Internships	\$52,000	\$0	\$8,000	\$52,000	Outreachy
Subtotal	\$257,781	\$17,952	\$8,758	\$239,829	

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

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

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>).