Technical Advisory Council (TAC) Meeting

March 23, 2023

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

Etherpad - Meeting Minutes

- https://etherpad.lfnetworking.org/p/CCC-TAC-Minutes-2023-03-23

- 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

CONFIDENTIAL COMPUTING CONSORTIUM

Agenda

1. Welcome, roll call, introduce any first-time attendees
2. Approval of minutes
3. Action item review
4. 2023 Goals
5. Tech Talk: SGX Assurance Tool (Alex Berenzon)
6. Project update: OE-SDK (Radhika Jandhyala)
7. Outreach:
    a. Event participation and LF diversity and inclusion policy
8. Any other business
    a. Project Progression
    b. Conformance to Terminology
    c. Community Architect Position
    d. Github Issue Cleanup

CONFIDENTIAL COMPUTING CONSORTIUM

Roll Call

Quorum requires **4** or more voting reps:

* *TAC chair*

Member	**Representative / Alternate**	**Email**
Accenture	Giuseppe Giordano	giuseppe.giordano@accenture.com
Arm	Thomas Fossati / Michael	thomas.fossati@arm.com
Meta Platforms	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	Lily Sturmann / Dimitrios	lsturman@redhat.com

Introduction of new attendees?

Approval of TAC Minutes

https://github.com/confidential-computing/governance/pull/159

Proposed:

That the minutes of the March 9, 2023 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. [Kurt] 1/12: Direct LF Creative to export the TAC whitepaper to markdown so we can put it under TAC source control.
    a. 1/26: Update request with LF Creative; 3/9: Copy/Paste problem fixed; Will submit PR(s) before 3/23 TAC meeting
    b. 3/22: Progress, but not clean to convert back to .md, will try editing source and getting help
2. [Howard] 1/12: Propose description in pull request for project state incubation requirements (target for after Chinese New Year)
    a. 3/9: Context: More mature lifecycle management.. facilitate more sandbox projects
    b. 3/23: [All] Please review https://github.com/confidential-computing/governance/pull/160; discuss next meeting.
3. [Alec/Dave] 1/26 : Board recommends a blog post explaining why we added attestation verbiage to CC definition.
    a. 2/9: Alec will sync with Dave / review meeting recording and start blog.
    b. 3/9: Underway. Will sync with Dave.
4. [Kurt/Helen] 2/9: work with the Gramine project (Mona V and Eric Voit) to plan website (cost problem ~6 months old)
    a. 2/28: Gramine updating previous brief for website
    b. 3/21: HL scheduled kickoff meeting for 3/30
5. [Dan/Kurt] 2/9: to look into a communication channel (mail list?) for discussing cross-project security concerns
    a. 3/9: No progress
    b. 3/21: Mail list created, need mentors to contact their projects for the right person to monitor
6. [Lily] 2/23: ask the Keystone project to get more specifics on their 1) test environment and runners 2) existing types of customization 3) repository overview 4) attestation IETF EAT implementation
7. [Kurt] 2/23: fix the Keystone website github link in the Contribute button (not the Github icon at the top) 3/23: (DONE)
8. [Mentors] 3/9: get input from their projects for project progression discussion in the next meeting
9. [Kurt] 3/9: pose the CCC Terminology enforcement question to the Governing Board for discussion
10. [Alec] 3/9: reach out to Mike for cleanup NVIDIA blog email
11. [Mark N] 3/9: agreed to take this plan forward in the GRC in April

CONFIDENTIAL COMPUTING CONSORTIUM

2023 TAC Goals

Working copy: https://docs.google.com/document/d/1BLsI0hv9ybHl-FBNqHp6bJzy6ng8yKs__556bTqBswc

“We have increased the impact of the CCC in the ecosystem such that…”

1. **we increased Cross-project Integration [Lily, EricV]**
2. **the CCC hosts s/w projects adopted by the ecosystem [Dave, Howard, Dan]**
3. **other organizations reference Confidential Computing [MarkN, Howard, Thomas]**
4. **grew outbound education [Dave, Nick, Giuseppe]**
5. **matured community D&I [Dan, Nick]**

<tbd> [Cfir, EricN]

CONFIDENTIAL COMPUTING CONSORTIUM

2023 TAC Goals

Working copy: https://docs.google.com/document/d/1BLsI0hv9ybHl-FBNqHp6bJzy6ng8yKs__556bTqBswc Update 1/26: Split out committees.

"We have increased the impact of the CCC in the ecosystem such that…"

1. **… we increased Cross-project Integration, adoption of common code, modules, patterns:**
    a. **There exists at least two CCC maintained modules which have been integrated by another CCC project during the year, as measured by being included as part of the installation process.**

    b. **The TAC sponsors at least one event with a primary goal cross-project integration which results in the attendance and active participation of code submitters from the majority of CCC projects.**

2. **… the CCC hosts s/w projects which fill key roles in the stack and are adopted by the ecosystem."**
    a. **One project has advanced its state of maturity – reflecting adoption by the ecosystem.**
    b. **Three new project communities joined rounding out our portfolio with an academic project, a new part of the stack (e.g. hypervisor), and a top level user interaction (or maybe something related to validation & conformance).**

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Tech Talk

- SGX Assurance Tool - Alex Berenzon

Project Annual Report

- OE-SDK - Radhika Jandhyala

CONFIDENTIAL COMPUTING CONSORTIUM

Outreach

- OC3 Items (March 15th)
  - CCC Sponsoring, Stephan Walli Keynote
  - Items to discuss
    -
- Outreachy Internships

Progression discussion

- What additional services do projects want?
  - Gramine: Website
  - Note that existing list came from project requests and voted in by TAC after original policy was created
  - Mentors check in with projects on wishlists
- Are different tiers / progression levels helpful or necessary?
  - History:
    - initial stage: is it defined enough to accept to the CCC
    - next stage: under development vs in production
  - How to apply criteria to projects with subprojects at different stages?

Conformance to Terminology

- Spreadsheet - Dave Thaler
  - Reactions to a recent post

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 Goal Topic	TAC Tech Talk
~~9 Feb 2023~~	~~Gramine - Michal, Mona, Woju~~		
~~23 Feb 2023~~	~~Keystone - Lily (Daycol)~~		~~AP-TEE - Ravi Sahita~~
~~9 Mar 2023~~			~~eBPF - Dave Thaler~~
23 Mar 2023	OE SDK - Radhika		SGX Assurance Tool - Alex Berenzon
6 April 2023	GRC - Mark Novak	Progression - Howard	CDCC - XiaoFeng Wang
20 April 2023		xProject - Lily / EricV	
4 May 2023		Education - Giuseppe et al	
18 May 2023	Veraison?		

Next Agenda (2023-04-06)

1. Welcome, roll call, introduce any first-time attendees
2. Approval of minutes
3. Action item review
4. 2023 Goals
5. Project Progression https://github.com/confidential-computing/governance/pull/160
6. Annual Report/Update: GRC SIG?
7. Tech Talk: CDCC - XiaoFeng Wang
8. Any other business
    a.
    b.

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	Lily	JUN 2021
Occlum	Ant Financial	20 AUG 2020	Yes	Yes	10 SEP 2020	15 SEP 2021	17 NOV 2022	Tate Tian	MAY 2021
Veracruz	Arm	3 SEP 2020	Yes	Yes	19 NOV 2020	14 APR 2021	18 NOV 2021	Thomas F	APR 2021
Veraison	Arm	4 FEB 2022	Yes	Yes	16 MAR 2022	18 May 2022	TBD	Howard Huang	NOV 2021

SIG / WG	Proposed by	TAC Approved	Tech. Charter	Board Presentation	Annual Review	Mentor	Webinar
CCC-Attestation SIG	TAC	Yes	Yes	18 MAR 2021	21 APR 2022	Dan	21 JUNE 2022
GRC SIG	TAC	Yes	Yes	21 SEP 2022	Quarterly	Mark Novak	

CONFIDENTIAL COMPUTING CONSORTIUM

Deferred topics / Backup

Conformance to terminology - Dave

Various examples across industry:

- IEC 62443
- Vendor self-assertion
- OCF: OCF-generated requirements and contracted certification
- IPv6Ready: IETF-generated requirements but external lab vendor certification
- DISA, NIST: Regulatory body requirements
- NISTIR 8259A: Regulatory body recommendations (not requirements)
- CCC Wikipedia article should follow TAC definitions
- …

Tentative TAC Tech Talk topics

- Trust domains - Mike?
- Defined-Trust Transport (DeftT) Protocol for Limited Domains - Kathleen Nichols, Van Jacobson, Randy King
- CDCC research updates
- Relationship between eBPF and Confidential Computing - Dave Thaler

TAC 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		

CONFIDENTIAL COMPUTING CONSORTIUM

Annual report

governance/project-progression-policy.md at main · confidential-computing/governance (github.com)

“The review includes the following:

1. Review whether any answers to the project's submission template or Technical Charter have changed, and if so, review the new answers. A representative from the project is responsible for presenting any deltas to the template answers since the last review, if any. If there are no changes, there is nothing to review here.
2. Review the project's progression status to determine whether the project is in the stage that accurately reflects its needs and goals. For example, is it already ready to move to another progression level? Is it on track at the current level? Is any action needed from the TAC (e.g., change in or addition to any project mentor(s))? If nothing has changed significantly, there may be nothing to review here.
3. Review any budget allocations relevant to the project, and whether any adjustments are needed.
4. Review license scans provided by the Linux Foundation. Provide feedback on any outstanding issues and evaluate the scanning service from the project's perspective.

Projects are encouraged to proactively inform the TAC when something changes that affects their submission template or Technical Charter (changing a License, security reporting process, CoC, etc.), rather than waiting for the next annual review.”

CONFIDENTIAL COMPUTING CONSORTIUM

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	

CONFIDENTIAL COMPUTING CONSORTIUM

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

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 $10K 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

Reference Common Test Infrastructure

- **Summary:**
  - Projects preferred per project funding. No demand for common infrastructure. Approvals retained here for reference.
- **Needing**:
  - LF IT ready to meet for sizing and technical requirements
- 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 ?? (Annual Report)**

Reference Common Test Infrastructure

- **Summary:**
  - Projects preferred per project funding. No demand for common infrastructure. Approvals retained here for reference.
- **Needing**:
  - LF IT ready to meet for sizing and technical requirements
- 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 ?? (Annual Report)**

CONFIDENTIAL COMPUTING CONSORTIUM