

Technical Advisory Council (TAC) Meeting

March 06, 2025



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. Old Business - Recap last meeting
3. Announcements
4. New Business
 - a. Annual Project Review:
 - Certifier Framework, John Manferdelli
 - b. TAC Discussion:
 - Project Liaison
 - Workload Identity?
 - OKRs
5. Future Business
 - a. Next meeting agenda
 -
 - b. Backlog

Roll Call

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

<u>Member</u>	<u>Representative / Alternate</u>	<u>Email</u>
AMD	Nathaniel McCallum / David Kaplan	Nathaniel.McCallum@amd.com
Arm	Paul Howard	Paul.Howard@arm.com
Google	Catherine Zhang	cxzhang@google.com
Huawei	Zhipeng (Howard) Huang	huangzhipeng@huawei.com
Intel	Dan Middleton * / Simon Johnson	dan.middleton@intel.com
Meta Platforms	Henry Wang / Kevin Hui	kevinhui@meta.com
Microsoft	Alec Fernandez	alfernandez@microsoft.com
Nvidia	Fritz Alder	falder@nvidia.com
Red Hat	Yash Mankad** / Ram Pai	ymankad@redhat.com
TikTok	Mingshen Sun / Dayeol Lee	mingshen.sun@tiktok.com
Shielded Technologies	Bob Blessing-Hartley	bob.blessing-hartley@shielded.io

* TAC chair

Welcome New Community Members

New to the community?

Haven't introduced yourself at least twice?

Let us know

- your name, pronouns
- where you are joining from
- your main Confidential Computing interest



© 2020 All rights reserved. All rights reserved.

Old Business

Last meeting:

1. Announcements
2. New Business
 - a. TAC Discussion:
 - Workload Identity, Mark Novak
 - Project Liaison
 - Governing Board Agenda item(s)
 - b. Tech Talk: Confidential Computing in the Age of AGI by Jacob Laggeros
3. Next Meeting agenda
4. Backlog

Announcements

- New TCA inbound
- Board meeting 2/26
 - The charter change was passed - Under legal review
- Trustworthy Workload Identity
 - New meeting schedule - See CCC Calendar
 - Draft Charter - Action items in the mail list
<https://lists.confidentialcomputing.io/g/tac/message/1468>

Annual Project Review

Certifier Framework by John Manfredelli

Project Liaisons

- <https://github.com/confidential-computing/governance/issues/207>
- 2024-05-02 “... DM stated that until we have a change of policy, each member of the TAC needs to sign up as a mentor. Various attendees of the meeting volunteered to mentor and the table was updated.”
- Things we might miss:
 - Generally connection with projects and TAC members,
 - Project Progression,
 - Sanctions discussion,
 - Annual reviews

TBD

Discussion:

Workload Identity
Mark Novak

TAC 2025 Objectives

- Projects

- All - Project Liaisons
- Mingshen
- Catherine

- Ecosystem

- Alec
- Nathaniel
- Paul

- Community

- Yash
- Fritz
- Mingshen

TBD:

- Howard
- Henry / Kevin

https://docs.google.com/document/d/1pa6XrOUhkIEFIP1MILtn_84OjxV12L5hogch0shJkaA/edit?tab=t.0

Projects

Project	Last Annual Review	Next Annual Review	Next Annual Review Date
Certifier Framework	2024-01-17	Q1	
Coconut-SVSM	2024-04-17	Q2	
Enarx	2024-04-04	Q2	
Gramine	2023-02-09	Q1	
Islet	2024-11-14	Q4	30 Oct
Keystone	2024-03-07	Q1	
ManaTEE	2024-07-25	Q3	
Occlum	2024-03-21	Q1	2025-3-20
OE SDK	2024-04-18	Q2	
SPDM-RS	2024-01-17	Q1	
Veracruz	2023-01-12	Q1	
Veraison	2024-08-08	Q3	
VirTEE	2024-01-17	Q1	

SIGs

Update

SIG / WG	Last Annual Review	Next Annual Review	Liaison
CCC-Attestation SIG	2022-04-21		Dan Middleton
GRC SIG	Quarterly 2023-10-08		Mark Novak
Kernel SIG	Launched Q1'24		Catherine Zhang - tentative

Topic Schedule 2025

Date	CCC Project Topic	TAC Goal Topic	TAC Tech Talk / Proposal / etc
2025-01-23	OpenVMM proposal, Caroline Perez-Vargas	Workload Identity - Mark Novak	Decentralized Storage Network, Łukasz Magiera
2025-02-06	Workload Identity	Introduce Project Liaisons topic (briefly)	1. Confidential Computing Carry-on, Jacob Laggeros 2. Secure Proxy, Jens Albers
2025-02-20	Workload Identity	Project Liaisons discussion; Board agenda	1. Jacob Laggeros now without fire. 15 mins to finish discussion.
2025-03-06			
2025-03-20		Intro to CC content (e.g. dev guide)	
2025-04-03			Why should we trust computing hardware/firmware? OCP-SAFE, Brayn Kelly - Requested 08:30 slot
2025-04-17			

Thank You



CONFIDENTIAL COMPUTING
CONSORTIUM