

Technical Advisory Council (TAC) Meeting

February 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
 - a. Fosdem, Tech Talks, US OFAC Sanctions
4. New Business
 - a. TAC Discussion:
 - Workload Identity, Mark Novak
 - b. Tech Talk:
 - Confidential Computing in the Age of AGI: with live demo, Jacob Laggeros
 - Secure Proxy, Jens Albers
5. Future Business
 - a. Next meeting agenda
 -
 - b. Backlog

Roll Call

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

* *TAC chair*

<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 / Yao Zhang	mingshen.sun@tiktok.com

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. Old Business
 - a. TAC Discussion:
 - Workload Identity, Mark Novak
 - b. Project Proposal:
 - OpenVMM by Caroline Perez-Vargas
 - c. Tech Talk:
 - Decentralized Storage Network, Łukasz Magiera
3. Next Meeting agenda
4. Backlog

Thanks:

- Mingshen,
- Fritz,
- Yash

for recent reviews of Minutes

Announcements

- Annual project updates - We shared the schedule early 2025 (Renu)
- Kernel SIG - Is schedule up? Coconut on agenda? (Catherine)
- Project Liaisons - Discussion next time (Dan)
 - Address shortage of Project Mentors [#207](#)
- US OFAC Sanctions - something for Liaisons to liaise? (Mike)
- Job board!!! See slack and web page is ready to go.
- Next page... Tech talks & FOSDEM (Fritz)

Tech Talks and FOSDEM recap

- 2025 Tech Talks - Help recruit directed topics:
 - Confidential AI
 - Securing Devices
 - Workload ID
 - others?
- Governance repo PR forthcoming.. scheduling FAQ
- FOSDEM Download

Discussion:

Workload Identity

Mark Novak





Tech Talk

Confidential Computing in the Age of AGI: with live demo
Jacob Laggeros



Tech Talk

Secure Proxy

Jens Albers

TAC 2025 Objectives

- Projects

- All - Project Liaisons
- Mingshen
- Catherine

- Ecosystem

- Alec
- Nathaniel
- Paul

- Community

- Yash
- Fritz
- Mingshen

TBD:

- Howard
- Henry / Kevin

Update

https://docs.google.com/document/d/1pa6XrOUhkIEFIP1MILtn_84QjxV12L5hogch0shJkaA/edit?tab=t.0

Projects

Project	Last Annual Review	Next Annual Review	Project Liaison
Certifier Framework	2024-01-17		
Coconut-SVSM	2024-04-17		Alec Fernandez
Enarx	2024-04-04		Nick Vidal
Gramine	2023-02-09		Eric V
Islet	2024-03-01		Bokdeuk Jeong
Keystone	2024-03-07		Lily Stuurman
ManaTEE	2024-07-25		Dayeol Lee
Occlum	2024-03-21		Tate Tian
OE SDK	2024-04-18		Alec Fernandez
SPDM-RS	2024-01-17		Fritz Alder
Veracruz	2023-01-12		Thomas Fossati
Veraison	2024-08-08		Howard Huang
VirTEE	2024-01-17		Yash Mankad

SIGs

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	1. Decentralized Storage Network, Łukasz Magiera
2025-02-06		Scrub Project Liaisons	1. Confidential Computing Carry-on, Jacob Laggeros 2. Secure Proxy, Jens Albers
2025-02-20			Need to get talk title, Brain
2025-03-06			
2025-03-20			
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