Technical Advisory Council (TAC) Meeting

Dec 11, 2025

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

Agenda

1. Welcome, roll call, introduce any first-time attendees
2. Old Business
3. Announcements
4. New Business
   a. Trustee - Helps address CC adoption hurdles - Ding Ma
   b. New TAC rule for 2026
   c. First 2026 deliverable
   d. Help fixup minutes
5. Future Business
   a. Discussion: CCC Responses to recent publications

CONFIDENTIAL COMPUTING CONSORTIUM

Roll Call

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

* *TAC co-chair*

Member	Representative / Alternate	Email
AMD	Nathaniel McCallum / David Kaplan	Nathaniel.McCallum@amd.com
Arm	Paul Howard	Paul.Howard@arm.com
Google	Rene Kolga / Keith Moyer	renekolga@google.com kmoy@google.com
Huawei	Wu Yongzheng	Wu.Yongzheng@huawei.com
Intel	Raynor Scott / Simon Johnson	scott.raynor@intel.com,simon.p.johnson@intel.com
Meta Platforms	Henry Wang / Kevin Hui	kevinhui@meta.com
Microsoft	Alec Fernandez	alfernandez@microsoft.com
Nvidia	Fritz Alder / Dan Middleton	falder@nvidia.com
Red Hat	Yash Mankad* / Ram Pai	ymankad@redhat.com
TikTok	Mingshen Sun	mingshen.sun@tiktok.com
Shielded Technologies	Bob Blessing-Hartley	bob.blessing-hartley@shielded.io

CONFIDENTIAL COMPUTING CONSORTIUM

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

CONFIDENTIAL COMPUTING CONSORTIUM

Old Business

1. 2026 Strategy
2. 2026 Budget

CONFIDENTIAL COMPUTING CONSORTIUM

Announcements

- Election results: Dan & Ijlal & you
- Next TAC meeting on January 08, 2026
- Board reduced overall budget including TAC.
  - Revisit funding proposals Jan 8.
  - Probably only afford 1 of https://github.com/confidential-computing/governance/issues/330

CONFIDENTIAL COMPUTING CONSORTIUM

New Business

Trustee - A general purpose attestation verifier and relying party services broker

- Useful independent of CNCF CoCo
- May help address our primary adoption hurdle

New TAC rule for 2026: https://github.com/confidential-computing/governance/pull/335

First deliverable(s) for 2026:
https://github.com/confidential-computing/governance/issues/336

Please help amend minutes:

https://github.com/confidential-computing/governance/pull/334

Thanks, Yash!

Thanks, Yash for your invaluable support as 2025 TAC Vice Chair.

And your leadership in the mentor program.

Discussion: Recent publications

Recent Publications:

- ANSSI Report
- TEE.fail; Battering RAM
- Gartner
- IDC Report

From last time…

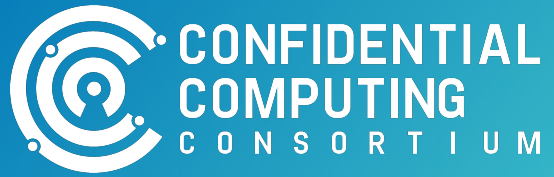
Issues:

- Standardization confusion
- Shared responsibility model un
- Physical security requirements
- Attestations out of context
- CC as soln vs. defense in depth
- Composite TEEs and attestations

Actions:

- ISO Liaison [Alec]
- Task Attestation SIG to define contextual attestation pattern [Keith]
- Global Platform / TCG engagement [Mike]
- Augment whitepapers for composite TEEs
- Schedule TAC session on IDC report [Dan]

Thank You



Projects

Project	Last Annual Review	Next Annual Review	Next Annual Review Date
Certifier Framework	2024-01-17	Q1	2025-03-06
Coconut-SVSM	2024-04-17	Q2	2025-06-12
Enarx	2024-04-04	Q2	2025-04-03
Gramine	2023-02-09	Q1	2025-04-17
Islet	2024-11-14	Q4	2025-10-30
Keystone	2024-03-07	Q1	2025-05-29
ManaTEE	2024-07-25	Q3	2025-08-07
Occlum	2024-03-21	Q1	2025-3-20
OE SDK	2024-04-18	Q2	2025-07-10
SPDM-RS	2024-01-17	Q1	2025-05-15
Veracruz	2023-01-12	Q1	2025-05-15
Veraison	2024-08-08	Q3	2025-09-18
VirTEE	2024-01-17	Q1	2025-3-20

CONFIDENTIAL COMPUTING CONSORTIUM

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

CONFIDENTIAL COMPUTING CONSORTIUM

Future Business

Update

1. Rotating co-leads for TAC meetings & OKR reviews
    a. Light agenda for rest of the year; we should do OKR reviews and CY26 planning

Date	Rotating Chair	CCC Project Topic	TAC Goal Topic
2025-09-18	Arm	Veraison	Arm OKR
2025-10-02	AMD	Conf AI SIG discussion / TWI + attestation discussion	AMD OKR
2025-10-16	Google	Attestation SIG update ?	Google OKR
2025-10-30	Huawei	Islet	Huawei OKR
2025-11-13	Intel		Intel OKR
2025-11-27	Microsoft		Microsoft OKR
2025-12-11	Nvidia		Nvidia OKR

2. GRC SIG Attendance
    a. Dedicated GRC topic at the TAC meeting
3. Confidential AI SIG discussion at next TAC call

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Maintenance

Glossary

https://github.com/confidential-computing/glossary

Minutes

https://github.com/confidential-computing/governance/pulls

TAC 2025 Objectives

- Projects
  - All - Project Liaisons
  - Mingshen
  - Catherine
- Ecosystem
  - Alec
  - Nathaniel
  - Paul
- Community
  - Yash
  - Fritz
  - Mingshen

TBD:

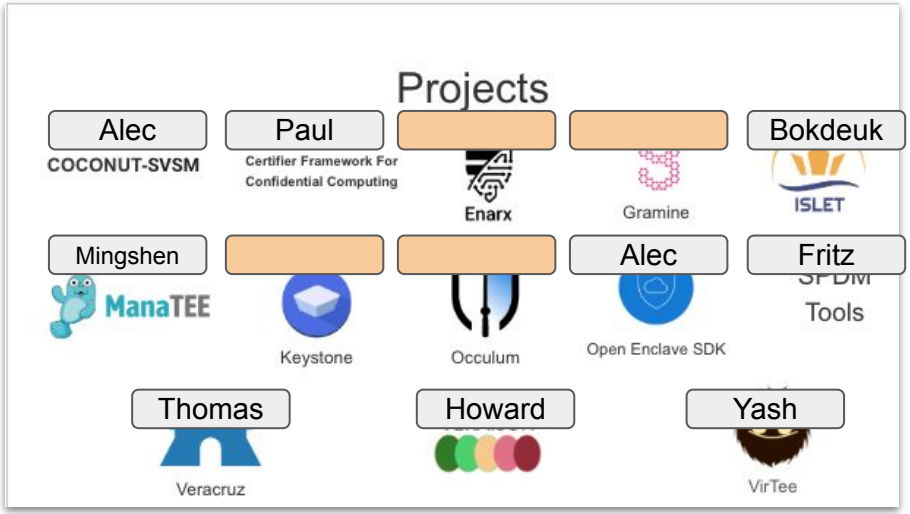
- Howard
- Henry / Kevin

https://docs.google.com/document/d/1pa6XrOUhkIEFIP1MlLtn_84OjxV12L5hogch0shJkaA/edit?tab=t.0

CONFIDENTIAL COMPUTING CONSORTIUM

Project Liaisons

Nathaniel
Henry
Bob



Dan	Catherine	Mark	Mark
Attestation	Kernel	GRC	TWI