Technical Advisory Council (TAC) Meeting

January 22, 2026

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. TAC expectations
   b. Revisit 2026 funding decision
   c. TAC Deliverable: Authoring Tech Guidance Docs
   d. Meeting Duration & Cadence
   e. TAC Tech Talk: Browser-based Remote Attestation, Rüdiger Kapitza
5. Future Business
   a. Next meeting agenda
   b.

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	Ahmed Magdy	ahmagdy@meta.com
Microsoft	Alec Fernandez / Simon Gallagher	alfernandez@microsoft.com / sgallagher@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. Trustee - Helps address CC adoption hurdles - Ding Ma
2. New TAC rule for 2026
3. First 2026 deliverable
4. Help fixup minutes

2025-10-15 Board Decision & TAC direction

“Transform the CCC into the acknowledged leader in creating and disseminating technical excellence for CC, promoting design best practice, use cases and reference architectures. Focus: best practice technical blueprints to service CC demand.”

1. **Mandate TAC** with best practices || reference architectures || open source project integration (TCA role cut)
2. Set up **Regulator-engagement SIG** under GB
3. **ED role priorities**
    a. Coordinate member engagements & Regulator SIG
    b. Recruit more members and do speaking engagements
    c. Aim for full 14 days/month average usage of ED (currently ~12.5)
4. **Reduce Outreach scope** and budget
5. OKRs for **members** for 2026

CONFIDENTIAL COMPUTING CONSORTIUM

Joint TAC & Board Member agreement on Basic Expectations & Q1 Deliverable

Agreed in Board meeting 2026/01/21

0. Subscribe to Maillist, Github, Slack
1. Attend and Contribute to TAC meetings
2. Rotating co-chair from voting Members - opportunity to shape agenda
3. Help define and create deliverables

Operating Procedures: https://github.com/confidential-computing/governance/pull/335/
Deliverable Proposal: https://github.com/confidential-computing/governance/issues/336

CONFIDENTIAL COMPUTING CONSORTIUM

Topic Schedule 2026

Date	Rotating Chair	CCC Project Topic	TAC Goal Topic	TAC Tech Talk / Proposal / etc
~~2026-01-08~~		~~no meeting~~		
2026-01-22	Just Dan & Ijlal	Project grant discussion in light of '26 re-budget	Guidance docs	Attested HTTPs Rudiger et al
2026-02-05	Nathaniel McCallum			
2026-02-19	Rene Kolga & Keith Moyer	OpenVMM		
2026-03-05	Wu Yongzheng			
2026-03-19	Scott Raynor			
2026-04-02	Ahmed Magdy	Enarx		
2026-04-16	Alec Fernandez	Gramine		
2026-04-30	Fritz Alder	COCONUT-SVSM		
2026-05-14	Yash Mankad / Ram Pai	Keystone		
2026-05-28	Bob Blessing-Hartley	SPDM-RS		

AL

U M

Revisit project allocations

The Board reduced our budget. We can afford one of these. Would anyone need to change their vote given we can afford 1 and not 2 of these?

https://github.com/confidential-computing/governance/issues/330

Votes taken 2025-11-13

Veraison PM: (6) Alec; Dan; Keith; Mingshen; Yash; Scott ⟵ Funded
SPDM Audit: (5) Alec; Dan; Keith; Mingshen; Yash ✖
Gramine Maintainer: (1) Scott ✖

Abstaining / Absent: Bob; Kevin; Nathaniel; Paul; Yongzheng;

CONFIDENTIAL COMPUTING CONSORTIUM

Strawman Deliverable

https://github.com/confidential-computing/governance/issues/336

Blueprint A: The Identity Bridge

- Attestation returns OpenID Connect token
- Connecting CC workloads to standard PaaS resources (SQL, Storage)

Blueprint B: The Secure Key Release

- KMS integration
- Encrypted resources

Blueprint C: The Collaborative Clean Room

- Multi-party
- Financial fraud detection, healthcare research, AI training

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Meeting Cadence

Historically: 2 hours every 2 weeks

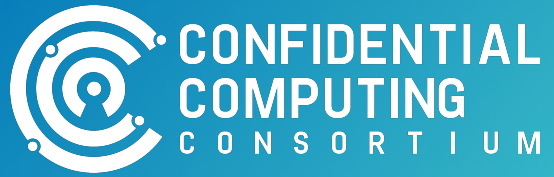
Currently: 1 hour every 2 weeks

Options:

- Status quo → Do more offline
- Return to 2 hours → Do more online
- Meet weekly for 1 hour → Do more online more frequently

CONFIDENTIAL COMPUTING CONSORTIUM

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	OpenVMM	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

Discussion: Recent publications

Recent Publications:

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

Previous Discussion

Issues:

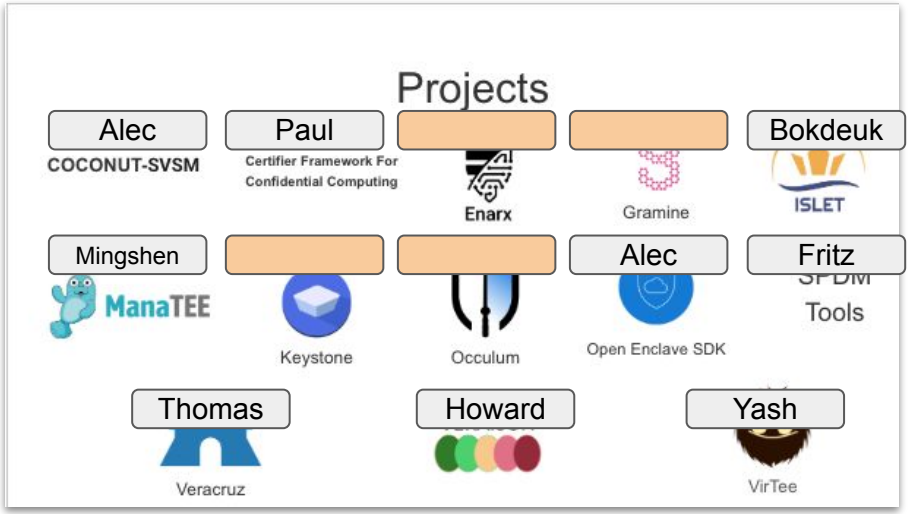
- Standardization confusion
- Shared responsibility model un
- Physical security requirements
- Attestations out of context
- CC as soln vs. defense in depth
- Composite TEEs and attestations

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]

Project Liaisons

Nathaniel
Henry
Bob



Dan	Catherine	Mark	Mark
Attestation	Kernel	GRC	TWI