Technical Advisory Council (TAC) Meeting

Oct 02, 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 - last 2 meetings canceled
3. Announcements
4. New Business
   a. ~~Nathaniel's OKR update~~ - Deferred
   b. Research Fund Committee
   c. 2026 Budget
   d. TikTok TAC Tech Talk: anonymous attestation project
5. Future Business
   a. Next meeting agenda
      - Dan's rotating (co-)chair proposal
   b. GRC SIG attendance

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	Catherine Zhang	cxzhang@google.com
Huawei	Wu Yongzheng	Wu.Yongzheng@huawei.com
Intel	Raynor Scott , Alternate -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

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. Annual Project review
    a. Veraison by Thomas & Simon
2. Paul’s OKR update
3. TikTok’s proposed Research Fund

CONFIDENTIAL COMPUTING CONSORTIUM

Announcements

- No announcements this week?

CONFIDENTIAL COMPUTING CONSORTIUM

TAC discussion:

Research Fund Proposal for Academic projects

Confidential Computing Consortium Research Fund

Need 2 volunteers besides TikTok to review proposals

CONFIDENTIAL COMPUTING CONSORTIUM

Budget planning for 2026

Budget Category	2025 Budget	Actuals	Forecast	Remaining	2026 Budget	Notes
TCA Travel	$15,000	$1,409	$0	$13,591	$20,000	
Travel	$14,000	$0	$0	$14,000	$14,000	~2k per project
Test Infrastructure	$45,500	$400	$16,968	$28,132	$45,000	~8.5k per project
Consortium IT Services and Tools	$14,950	$2,364	$0	$12,586	$15,000	~1.4k per project
Mentorship	$32,000	$0	$0	$32,000	$18,000	
	$121,450	**$4,173**	**$16,968**	**$100,309**	**$112,000**	

2 Big Ticket Items for discussion

Technical Community Architect: $100k → [0, $200k]
SPDM security audit: $70k

CONFIDENTIAL COMPUTING CONSORTIUM

TCA Role

Project	Annual Review Date	Blog	Open SSF Score Card	Practices Score (all scores 'owned' by Sal Kimmich available here)	OpenSSF Best Practices Badge ID	2024 Project Demo	Most Recent Demo	Mentorship Program	Mentorship Program Communication Issue #
COCONUT_SVSM		Next Blog /	7.3	100%	passing	Securin…	Coconut SVM 2024 Demo		https://github.com/coconut-svsm/svsm/issues/395
Certifier_Framework		Potential for post CC S Blog	5.2	84%	passing 84%			23, 9:24 AM (4 framework-for-c uested Chris to	https://github.com/ccc-certifier-framework/certifier-framework-for-confidential-computing/iss
Enarx			5.1	100%	passing		Enarx Demo 2021		Enarx - left message on community support chat (only supports bug reports)
Gramine			6	100%	passing		Gramine Demo 2022		moved to discussion: https://github.com/gramineproject/gramine/discussions/1926
Islet		Potential for post CC S Blog	5.8	67%	in progress 67%			Interest for Aug	https://github.com/islet-project/islet/issues/340
Keystone			4	49%	In progress 49%		Keystone Demo		https://github.com/keystone-enclave/keystone/issues/453
Occlum		Potential for post CC S Blog	4.8	85%	In Progress 85%				https://github.com/occlum/occlum/issues/1578
Open_Enclave_SDK			6	75%	In progress 75%		Open Enclave SDK Demo 2021		https://github.com/openenclave/openenclave/issues/4998
Veracruz			4.8	67%	pr not merged		Veracruz 2021 Demo		https://github.com/veracruz-project/veracruz/issues/672
Veraison			5.6	91%	e last 4% when they		Veraison Demo 2022		https://github.com/veraison/services/issues/238
VirTEE			5.2	43%	In progress 43%				https://github.com/virtee/sev/issues/199
ManaTEE			3.7		Created, 49%				
spdm-rs			7.4	97%	In progress 97%				https://github.com/ccc-spdm-tools/spdm-rs/issues/108

- DevRel with Projects
- Blog Posts
- Conference Support

CONFIDENTIAL COMPUTING CONSORTIUM

Topic Schedule 2025

Date	Rotating Chair	CCC Project Topic	TAC Goal Topic
2025-09-18	~~Arm~~	Veraison	~~Arm~~
2025-10-02	~~AMD~~		Budget; TCA; Sec analysis; Research committee

CONFIDENTIAL COMPUTING CONSORTIUM

Future Business

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

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	2025-07-10
Occlum	2024-03-21	Q1	2025-3-20
OE SDK	2024-04-18	Q2	2025-06-26
SPDM-RS	2024-01-17	Q1	2025-05-15
Veracruz	2023-01-12	Q1	2025-05-01
Veraison	2024-08-08	Q3	2025-09-04
VirTEE	2024-01-17	Q1	2025-3-20

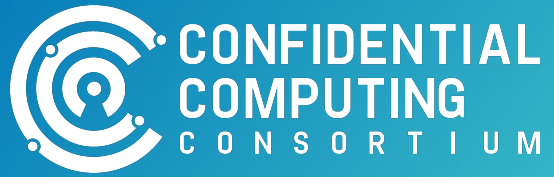
CONFIDENTIAL COMPUTING CONSORTIUM

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

Thank You



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:

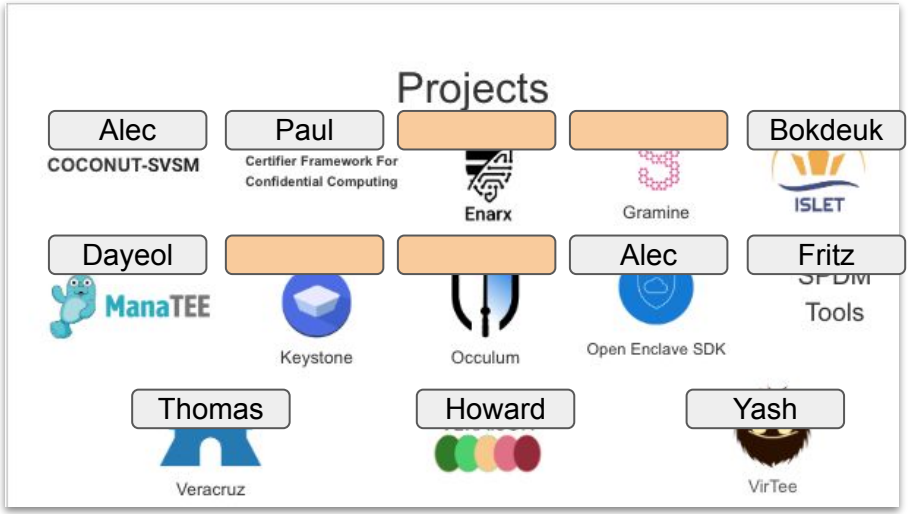
- Howard
- Henry / Kevin

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