Technical Advisory Council (TAC) Meeting

April 17, 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 - Recap last meeting
3. Announcements
4. New Business
   a. TAC Discussion:
      - Gramine: Annual project update
      - Security Baseline: Open discussion
      - GRC SIG Document review
      - OC3 recap
5. Future Business
   a. Next meeting agenda
   b. Backlog

CONFIDENTIAL COMPUTING CONSORTIUM

Roll Call

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

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	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*

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

Last meeting:

1. Announcements
    a. GB meeting, OC3 recap volunteer

2. Old Business
    a. TAC Discussion:
        - Enarx - Annual project update
        - ISO - Alec
        - Security Baseline intro - Emily Fox
        - Liaison check-in (time permitting)

    b. Tech Talk:
        - Why should we trust computing hardware/firmware? - Bryan Kelly

CONFIDENTIAL COMPUTING CONSORTIUM

Announcements

- RSA Conference
  - CCC Booth slots available

- Board meeting 4/23
  - Topics?

CONFIDENTIAL COMPUTING CONSORTIUM

Annual Project Review

Gramine

GRC SIG Document review

CONFIDENTIAL COMPUTING CONSORTIUM

Security Baseline: Open discussion

CONFIDENTIAL COMPUTING CONSORTIUM

OC3 recap

CONFIDENTIAL COMPUTING CONSORTIUM

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	Certifier Framwork	Project Liaisons	
2025-03-20	VirTEE, Occlum; Veracruz EOL	TWI SIG proposal	
2025-04-03	Enarx	Security Baseline intro - Emily Fox 11:00 -11:30	Why should we trust computing hardware/firmware? OCP-SAFE, Bryan Kelly - Requested 08:30 slot
2025-04-17	Gramine	GRC SIG Document review	
2025-05-01	Veracruz - vote to move to Emeritus		
2025-05-15	spdm-rs		
2025-05-29	Keystone		
2025-06-12	COCONUT_SVSM		Ravi Sahita - RISC-V CoVE update
2025-06-26	Open_Enclave_SDK	Intro to CC content (e.g. dev guide), CC Summit recap	

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

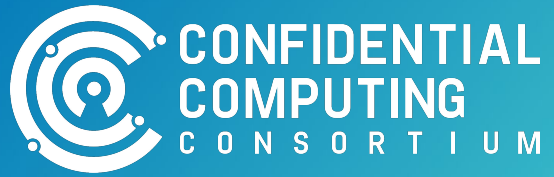
CONFIDENTIAL COMPUTING CONSORTIUM

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 2025 Objectives

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

TBD:

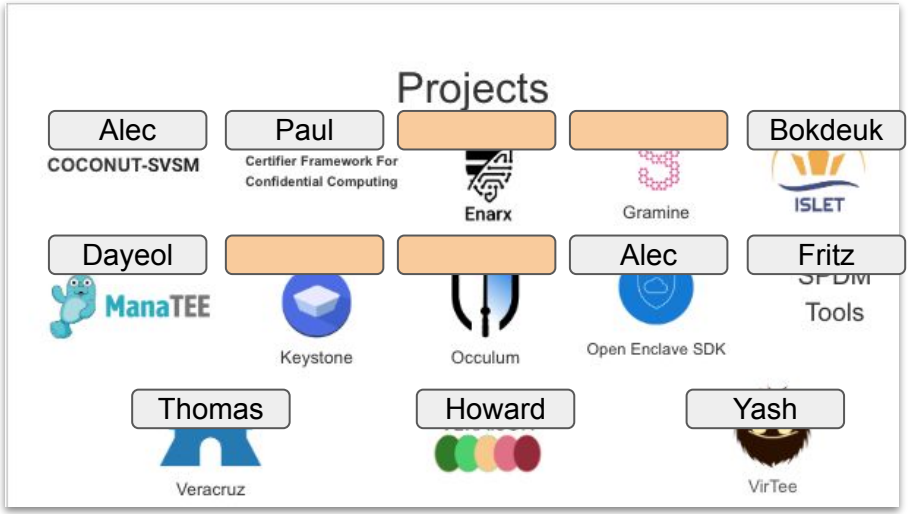
- Howard
- Henry / Kevin

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