

Technical Advisory Council (TAC) Meeting

October 17, 2024



CONFIDENTIAL COMPUTING
CONSORTIUM

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. Kubecon activities
 - b. TAC Chair Election
 - c. Face to face at FOSDEM
4. New Business
 - a. CC Brand Repositioning WG Update
 - b. Budget Update and 2025 Budget
 - ~~c. Tech Talk: Linux Plumbers Conf. recap?~~
5. Future Business
 - a. Next meeting agenda
 - OKR updates - ALL TAC MEMBERS
 - b. Backlog
 - 2025 Planning

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



Old Business

Last meeting:

1. Tech Talk - Chandra Nelogal
 - a. Extending Confidentiality to Data Storage
2. Tech Talk - Caroline Perez-Vargas
 - a. Open HCL
3. Attestation Terminology

Announcements

KubeCon Salt Lake City

CCC have a booth at Kubecon and a lot of incredible CC coverage this year.
([tentative full schedule available here](#)).

Booth Coverage is complete! Final schedule, talks and mini sessions will be sent to the mailing list today, and are represented on our “Confidential Computing Power User Bingo” style and complete schedule available now.
[Direct link to view and edit available here.](#)




CONFIDENTIAL COMPUTING CONSORTIUM

Here's your own personal **CCC Power bingo card**—a great way to explore the forefront of Confidential Computing (CC) at KubeCon! Equipped with your special card listing all the must-see mini sessions at our booth and talks at this conference, you can embark on a journey through cutting-edge discussions and hands-on demonstrations.

Whether you're navigating the complexities of data privacy in large-scale compute environments or delving into the nuances of serverless GPU cloud functions, this is your gateway to mastering the art of confidentiality in cloud-native computing. **Ready, set, discover.**






CONFIDENTIAL CONTAINERS 101: A HANDS-ON WORKSHOP MICROSOFT WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST	CONFIDENTIAL COMPUTE: A USE CASE MINI SESSION RED HAT WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST	FROM SILICON TO SERVICE: ENSURING CONFIDENTIALITY IN SERVERLESS GPU CLOUD FUNCTIONS NVIDIA WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST
CONFIDENTIAL COMPUTE: CONFIDENTIAL COLLABORATIVE AI ULTRAVIOLET WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST	GPU	REMOTE ATTESTATION USING VERASION: LIVE 10 MINUTE OPEN SOURCE PROJECT DEMO LINARO WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST
REMOTE ATTESTATION - THE KEY INGREDIENT FOR CONFIDENTIAL COMPUTING ANJUNA SECURITY WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST	PRIVACY IN THE AGE OF BIG COMPUTE CONFIDENTIAL COMPUTING CONSORTIUM WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST	PROTECTING LLMs WITH CONFIDENTIAL COMPUTING ULTRAVIOLET WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST

Confidential Computing protects data in use by performing computation in a hardware-based, attested Trusted Execution Environment. These secure and isolated environments prevent unauthorized access or modification of applications and data while in use, increasing the security assurances for organizations that manage sensitive and regulated data. **Turn over to learn more!**



CONFIDENTIAL COMPUTING CONSORTIUM

You can complete your **CCC Power User** visit the Confidential Computing Consortium booth during KubeCrawl to engage directly with experts, participate in discussions, and pick up cool swag. Explore a wealth of resources on the CCC website to fulfill other bingo squares from the comfort of your own device, and **join us during KubeCrawl 2024 to win prizes!**

VISIT THE BOOTH TO LEARN MORE ABOUT REMOTE ATTESTATION CCC BOOTH Q35	CONFIDENTIAL COMPUTE: A USE CASE MINI SESSION RED HAT WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST	PET JEOPARDY: THE PRIVACY ENHANCING TECHNOLOGY KNOWLEDGE GAME WED, 12-12-24 - 12-12-24 12:00PM - 12:00PM EST
CCC STAFF AND MEMBER Q&A WITH SWAG GIVEAWAY CONFIDENTIAL COMPUTING		LEARN MORE ABOUT CCC SPECIAL INTEREST GROUPS 
LEARN ABOUT CCC OPEN SOURCE PROJECTS 	READ THE 2024 CONFIDENTIAL COMPUTING USE CASE REPORT 	LEARN ABOUT CCC MEMBERSHIP BENEFITS 

TURN OVER FOR EVEN MORE WORKSHOPS, TALKS AND MINI SESSIONS ON CONFIDENTIAL COMPUTING AT KUBECON

Announcements

KubeCon Asset Side 1: KubeCon Talks and Workshops on Confidential Computing

1. **From Silicon to Service: Ensuring Confidentiality in Serverless GPU Cloud Functions (NVIDIA)**
 - **Time:** Thu. 11:00 AM - 11:35 AM, **Location:** Salt Palace | Level 1 | 151 G
2. **Privacy in the Age of Big Compute (Confidential Computing Consortium)**
 - **Time:** Fri. 4:00 PM - 4:35 PM, **Location:** Salt Palace | Level 1 | Grand Ballroom A
3. **Confidential Containers 101: A Hands-on Workshop (Microsoft)**
 - **Time:** Wed. 2:30 PM - 4:00 PM, **Location:** Salt Palace | Level 1 | Grand Ballroom G
4. **Remote Attestation Using Veraison: Live 10 Minute Open Source Project Demo (Linaro)**
 - **Time:** Wed. 10:45 AM - 12:45 PM, Thu. 10:45 AM - 12:45 PM, **Location:** CCC Booth Q25
5. **Confidential Compute: A Use Case Mini Session (Red Hat)**
 - **Time:** Wed. 6:00 PM - 6:30 PM, Thu. 2:30 PM - 4:30 PM, **Location:** CCC Booth Q25
6. **Confidential Collaborative AI (Ultraviolet), Time:** Wed. 4:00 PM - 4:30 PM, **Location:** CCC Booth Q25
7. **Protecting LLMs with Confidential Computing (Ultraviolet)**
 - **Time:** Thu. 4:30 PM - 5:00 PM, **Location:** CCC Booth Q25
8. **Security Mini-Talk on Remote Attestation (Anjuna)**
 - **Time:** Wednesday, 2:45 PM – 3:15 PM, **Location:** CCC Booth Q25

Announcements

KubeCon Slide 2 Highlights Booth Engagement and Online Resources

Side 2 - During KubeCrawl Highlights Booth Engagement and Online Resources

1. **Confidential Compute: A Use Case Mini Session (Red Hat)**
 - **Time:** Wed. 6:00 PM - 6:30 PM,
 - **Location:** CCC Booth Q25
2. **Jeopardy: The Privacy Enhancing Technology Knowledge Game**
 - **Time:** Wed. 7:00 PM - 7:30 PM,
 - **Location:** CCC Booth Q25
3. **Q&A with Swag Giveaway**
 - **Time:** During KubeCrawl, **Location:** CCC Booth Q25
4. **Security Mini-Talk on Remote Attestation Anjuna**
 - **Time:** Wednesday, 2:45 PM – 3:15 PM
5. **QR Code to Online Engagement: 1) OS Projects, 2) SIGs 3) Membership Benefits and 4) Use Case Report**



CONFIDENTIAL COMPUTING CONSORTIUM

Side 1

Here's your own personal **CCC Power bingo card**—a great way to explore the forefront of Confidential Computing (CC) at KubeCon! Equipped with your special card listing all the must-see mini sessions at our booth and talks at this conference, you can embark on a journey through cutting-edge discussions and hands-on demonstrations.

Whether you're navigating the complexities of data privacy in large-scale compute environments or delving into the nuances of serverless GPU cloud functions, this is your gateway to mastering the art of confidentiality in cloud-native computing. **Ready, set, discover.**

**CONFIDENTIAL
CONTAINERS 101: A
HANDS-ON
WORKSHOP**

MICROSOFT
WED. 12:00 - 12:30
LEVEL 2
GRAND BALLROOM D

**CONFIDENTIAL
COMPUTE:
A USE CASE
MINI SESSION**

RED HAT
WED. 12:00 - 12:30
THU. 12:00 - 12:30
CCC Booth Q25

**FROM SILICON TO
SERVICE: ENSURING
CONFIDENTIALITY IN
SERVERLESS GPU
CLOUD FUNCTIONS**

NVIDIA
WED. 11:00 - 11:25
LEVEL 3 1ST F

**CONFIDENTIAL
COMPUTE:
CONFIDENTIAL
COLLABORATIVE AI**

ULTRAVIOLET
WED. 12:00 - 12:30
CCC Booth Q25



**REMOTE
ATTESTATION USING
VERAISON:
LIVE 10 MINUTE OPEN
SOURCE PROJECT DEMO**

LINARO
WED. 12:45 - 12:45
THU. 12:45 - 12:45
CCC Booth Q25

**REMOTE
ATTESTATION - THE
KEY INGREDIENT
FOR CONFIDENTIAL
COMPUTING**

ANJUNA SECURITY
WED. 12:45 - 12:45
CCC Booth Q25

**PRIVACY IN THE
AGE OF BIG
COMPUTE**
CONFIDENTIAL
COMPUTING
CONSORTIUM

WED. 12:00 - 12:00
LEVEL 2
GRAND BALLROOM D

**PROTECTING
LLMS WITH
CONFIDENTIAL
COMPUTING**

ULTRAVIOLET
THU. 12:00 - 12:00
CCC Booth Q25

Confidential Computing protects data in use by performing computation in a hardware-based, attested Trusted Execution Environment. These secure and isolated environments prevent unauthorised access or modification of applications and **data while in use**, increasing the security assurances for organisations that manage sensitive and regulated data. **Turn over to learn more!**



CONFIDENTIAL COMPUTING CONSORTIUM

Side 2

You can complete your **CCC Power User visit** the Confidential Computing Consortium booth during KubeCrawl to engage directly with experts, participate in discussions, and pick up cool swag. Explore a wealth of resources on the CCC website to fulfill other bingo squares from the comfort of your own device, and **join us during KubeCrawl 2024 to win prizes!**

**VISIT THE BOOTH
TO LEARN MORE
ABOUT REMOTE
ATTESTATION**
**CCC BOOTH
Q25**

**CONFIDENTIAL
COMPUTE:
A USE CASE
MINI SESSION**
RED HAT
WED. 12:00 - 12:30
DURING KUBECRAWL
CCC Booth Q25

**PET JEOPARDY:
THE PRIVACY
ENHANCING
TECHNOLOGY
KNOWLEDGE GAME**
WED. 12:00 - 12:30
DURING KUBECRAWL
CCC Booth Q25

**CCC STAFF AND
MEMBER
Q&A WITH SWAG
GIVEAWAY**

DURING KUBECRAWL
CCC Booth Q25



**LEARN MORE
ABOUT CCC
SPECIAL INTEREST
GROUPS**



**LEARN ABOUT CCC
OPEN SOURCE
PROJECTS**



Also at CCC Booth Q25

**READ THE 2024
CONFIDENTIAL
COMPUTING USE
CASE REPORT**



Also at CCC Booth Q25

**LEARN ABOUT CCC
MEMBERSHIP
BENEFITS**



Online Access

**TURN OVER FOR EVEN MORE WORKSHOPS, TALKS
AND MINI SESSIONS ON CONFIDENTIAL COMPUTING AT KUBECON**

Announcements

- The **Technical Advisory Committee elections** will take place in November
- We need nominees for the Committee Chair for 2025
- All premier members reps are eligible vote for candidates
- More information to follow in on the TAC mailing list

Announcements

FOSDEM February 1-2 @ Brussels

- Interest in face to face at FOSDEM from Attestation SIG.
- What about TAC?

CC Brand Repositioning WG Update

October 17, 2024

CC Brand WG Key Updates

WG meeting Oct. 9:

- The WG completed first draft of the messaging guide and marketing message.
 - Seeking feedback from this TAC meeting.
 - Next on the milestone is to address feedback and present second version presented to the Governing Board by October 23. Final deliverable targeted for December 1.
- Analyst reports & engagement:
 - Discussed and continued to review the proposal and scope with IDC for the custom survey project.
- The WG shared insights from PSR conference, highlighting the use cases covered and emerging regulatory trends.

TAC September Discretionary Budget Update

Budget Category	2024 Budget	Actuals	Forecast	Remaining
TCA Travel	\$45,500	\$7,950	\$0	\$37,550
Travel	\$14,000	\$6,584	\$0	\$7,416
Test Infrastructure	\$59,500	\$1,212	\$4,500	\$53,788
Consortium IT Services and Tools	\$9,996	\$0	\$0	\$9,996

TAC Budget Proposal 2025

Budget Category	2024 Budget	Actuals	Forecast	Remaining	2025 Budget
TCA Travel	\$45,500	\$7,950	\$0	\$37,550	\$20,000
Travel	\$14,000	\$6,584	\$0	\$7,416	\$14,000
Test Infrastructure	\$59,500	\$1,212	\$4,500	\$53,788	\$45,000
Consortium IT Services and Tools	\$9,996	\$0	\$0	\$9,996	\$0
Mentorship	\$32,000	\$0	\$1,500	\$30,500	\$18,000
	\$160,996	\$15,746	\$6,000	\$139,250	\$97,000

Open Items: Lab .. Virtual or Physical providing bare metal access to Projects, Universities, member companies?

Consider project portfolio growth

Tech Talk

Linux Plumbers Conf. recap

Attestation & AVS questions

- New business models document
 - Major re-write
 - Focused on business, not technical
- Take a look here
 - <https://docs.google.com/document/d/1XzOZJ3qfP4xAb8j3YtqYdYMI50oPAyyY59yLVpHHcik/edit#heading=h.1cwejrnpvn82>
 - Remember: please keep comments on the **business** side
 - Feel free to share with colleagues

Attestation & AVS questions

Business models doc encouraged lots of discussion. Key technical questions:

- Do we need to add “remote” to the CCC definition of CC? (*Consensus: yes, but...*)
 - ...do we need to work with IETF to define remote attestation better?
- Define:
 - Attestation Verification Service (AVS)
 - **Workload ← Re-opened at Attestation SIG**
 - Endorsement, endorser
 - TEE
 - ...
- AVS-specific
 - What service characteristics are MUST/SHOULD/MAY for an AVS to provide
 - Are there use cases to run an AVS which is not workload-aware?
 - Describe different policies that might be relevant to an AVS
 - AVS trust relationships:
 - How can an AVS prove that it should be trusted?
 - OR What evidence should a relying party accept to establish a trust relationship to an AVS?
- **What entities may a relying party wish to remove from their trust chain? ← Mail List discussion**
- **BONUS:** Clear need to describe and classify different models for CC with Linux Containers

Attestation & AVS questions

What entities may a relying party wish to remove from their trust chain? ← **Mail List discussion**

Subtext?: What if the CSP operates the AVS?

Variants: Is the CSP in ~~the~~ TCB your trust boundary? How much of the CSP? Can I have my Managed Services and eat them too?

Mail list: Turtles / CSP->Auditor; Separation of Duties;

Approaches to Enumerating the Entities:

Enumerate Software: Attestation Values: Services/Operational Roles:

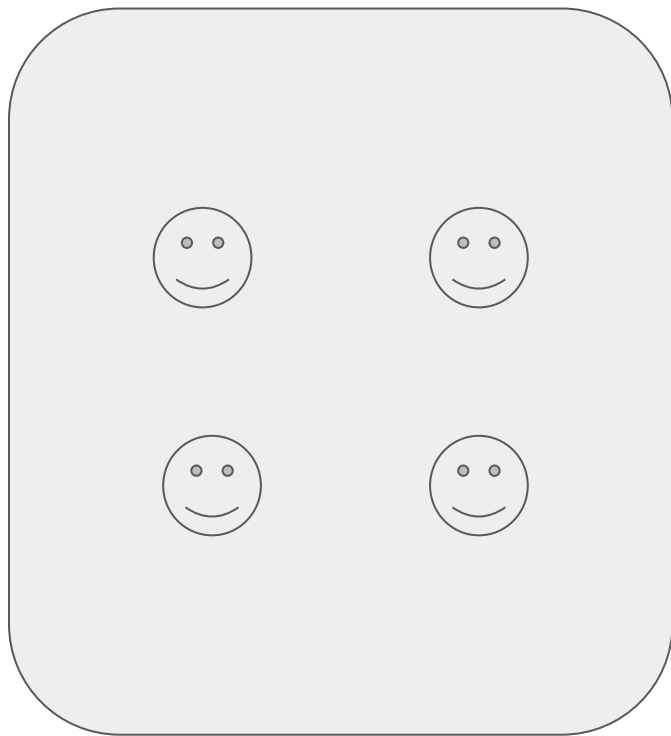
IAAS

PAAS

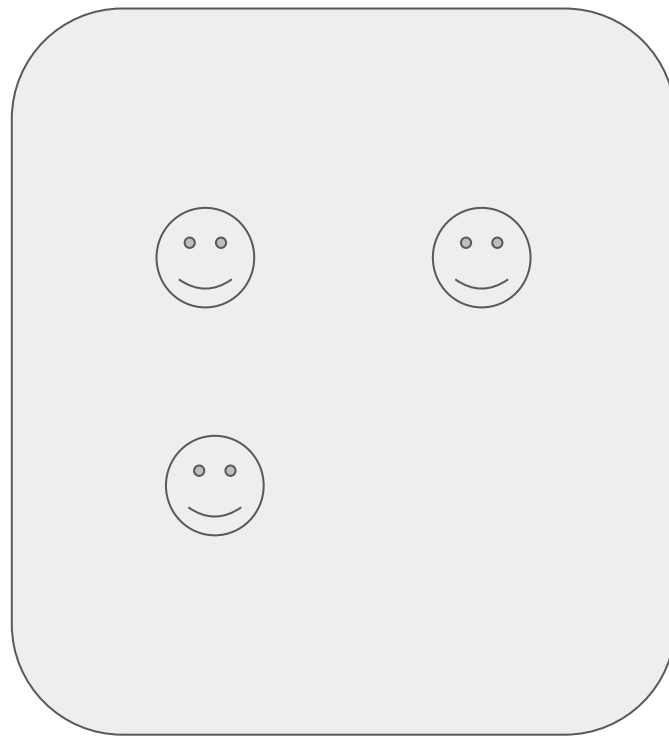
SAAS

FAAS

Without CC



With CC



Can we get to a description like this?

Projects

Project	Last Annual Review	Next Annual Review	Project Liason	Webinar	
Enarx	2024-04-04		Nick Vidal	Jan 2021	added to invite
OE SDK	2024-04-18		Alec Fernandez	Mar 2021	added to invite
Gramine	2023-02-09		Eric V	Feb 2022	
Keystone	2024-03-07		Lily Stuurman	Jun 2021	added to invite
Occlum	2024-03-21		Tate Tian	May 2021	requested
Veracruz	2023-01-12		Thomas Fossati	Apr 2021	
Veraison	2023-06-13	2024-08-08	Howard Huang	Nov 2021	Invitation accepted
VirTEE	2024-01-17		Yash Mankad		
SPDM-RS	2024-01-17		Fritz Alder		
Certifier Framework	2024-01-17				
Islet	2024-03-01		Bokdeuk Jeong		
Coconut-SVSM	2024-04-17		Alec Fernandez		

SIGs

SIG / WG	Last Annual Review	Next Annual Review	Liason	Webinar
CCC-Attestation SIG	2022-04-21		Dan	21 June 2022
GRC SIG	Quarterly 2023-10-08		Mark Novak	
Kernel SIG	Launched Q1'24		Catherine Zhang - tentative	

Topic Schedule

Date	CCC Project Topic	TAC Goal Topic	TAC Tech Talk / Proposal / etc
2024-07-25	Data Clean room cont.	Catherine Zhang (Kernel SIG - Rebranding? Conformance?)	Post Quantum - Hart Montgomery; AI / OPEA Zhiwei Zhang
2024-08-08		Fritz Alder (Academia & Tech Talks)	Runtime Attestations - Jason Rogers - Invary
2024-08-22	Tech Talk: OPEA project	Mingshen Sun / Yao Zhang (TBD)	Pandora: Principled Symbolic Validation of Intel SGX Enclave Runtimes (Jo Van Bulck)
2024-09-05		Yash Mankad / Ram Pai (Mentorship)	Super Tech Talk - Andrey Pogoreltsev - CTO of Super Protocol
2024-09-19	Linux Plumbers conflicts?	?	- Collaborative and Private Data Processing with TEE-enforced Sticky Policy (Zhiqiang Lin) - Research topic: Formal programming techniques for secure data processing by Patrick Eugster
2024-10-03	Rosh Hashanah conflicts?	?	- Chandra Nelogal: Extending Confidentiality to Data Storage - Caroline Perez-Vargas: Project presentation
2024-10-17		David Kaplan (Plumbers recap)	
2024-10-31		OKR Updates - ALL TAC MEMBERS	2025 Planning
2024-11-14		2025 Planning	
2024-11-28	US Thanksgiving Conflicts	Cancel	Cancel

Thank You



CONFIDENTIAL COMPUTING
CONSORTIUM