Technical Advisory Council (TAC) Meeting

Sep 18, 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.

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. Annual Project review
        - Veraison by Thomas & Simon
    b. Paul’s OKR update
    c. TikTok’s proposed Research Fund
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. Meeting after ~6 weeks (8/21 and 9/4 meetings were canceled)
2. Dstack project proposal - approved!
3. Glossary - Deferred

CONFIDENTIAL COMPUTING CONSORTIUM

Announcements

- Veraison mentorship is now live:
  - https://mentorship.lfx.linuxfoundation.org/project/a779bae4-dc15-402b-ba2d-3fda6523c3ce

- Compliance page is now live: https://confidentialcomputing.io/resources/compliance/

Annual Project Review: **Veraison** by Simon Frost

2025 TAC Objective Review:

Arm’s Ecosystem OKR by Paul Howard

Ecosystem OKR 2025

Objective: We have helped to educate developer communities on confidential computing concepts

Key Results:

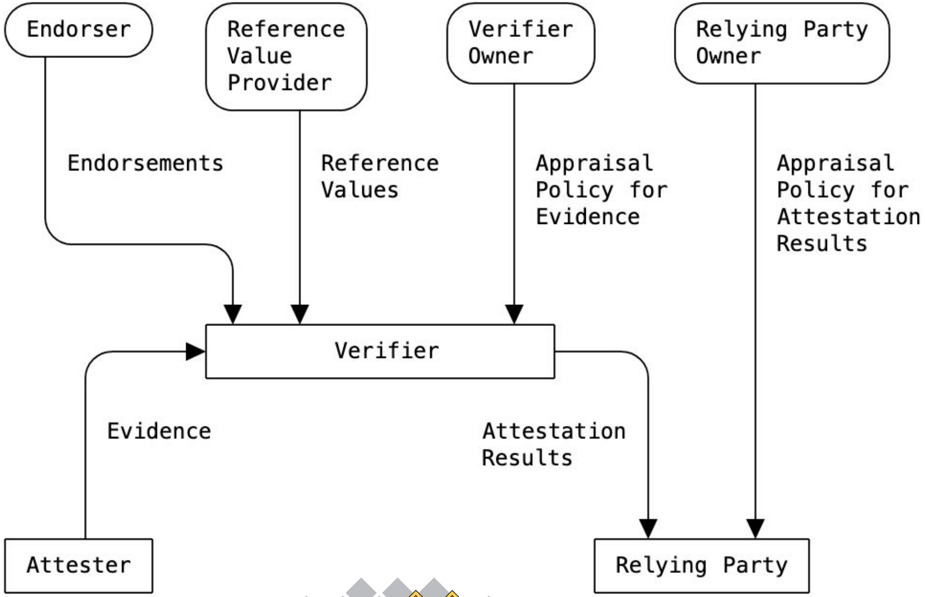
- Reusable software components are available in open-source, enabling developers to gain **hands-on** familiarity with core concepts **such as attestation**, in a digestible and approachable way
- Presentation materials are available (documents, videos, tutorials) to provide guided walk-throughs of how to build/run demonstrations

Focus on Attestation Because…

- It's a defining characteristic of confidential computing, therefore both ubiquitous and critical - an essential thing to understand
- It's complicated!
- Spans multiple components with different roles and interactions
- Happens at different times
  - Boot, workload deployment, data delivery, secure channel establishment
- Is fragmented, but with standards emerging
- Conceptual overviews exist, but then there's a big jump up to coding in production systems
- We have Veraison! 🩷

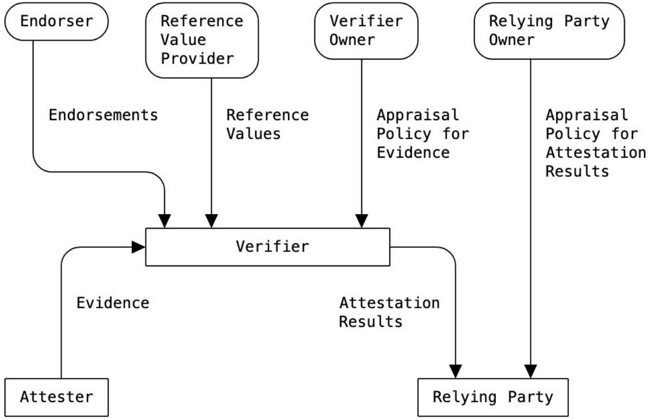
CONFIDENTIAL COMPUTING CONSORTIUM

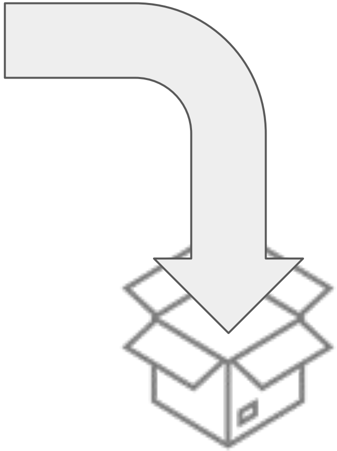
RATS Architecture as an Educational Model



- Generic and agnostic model based on abstract roles and interactions
- Establishes a common language and thought model
- Nurtured by the RATS Working Group within IETF, hence also the basis for standards
- Looks uniform at all scales and for all use cases
- But… it's only a model, it's not an implementation

“RATS in a Box” Developer Experiences

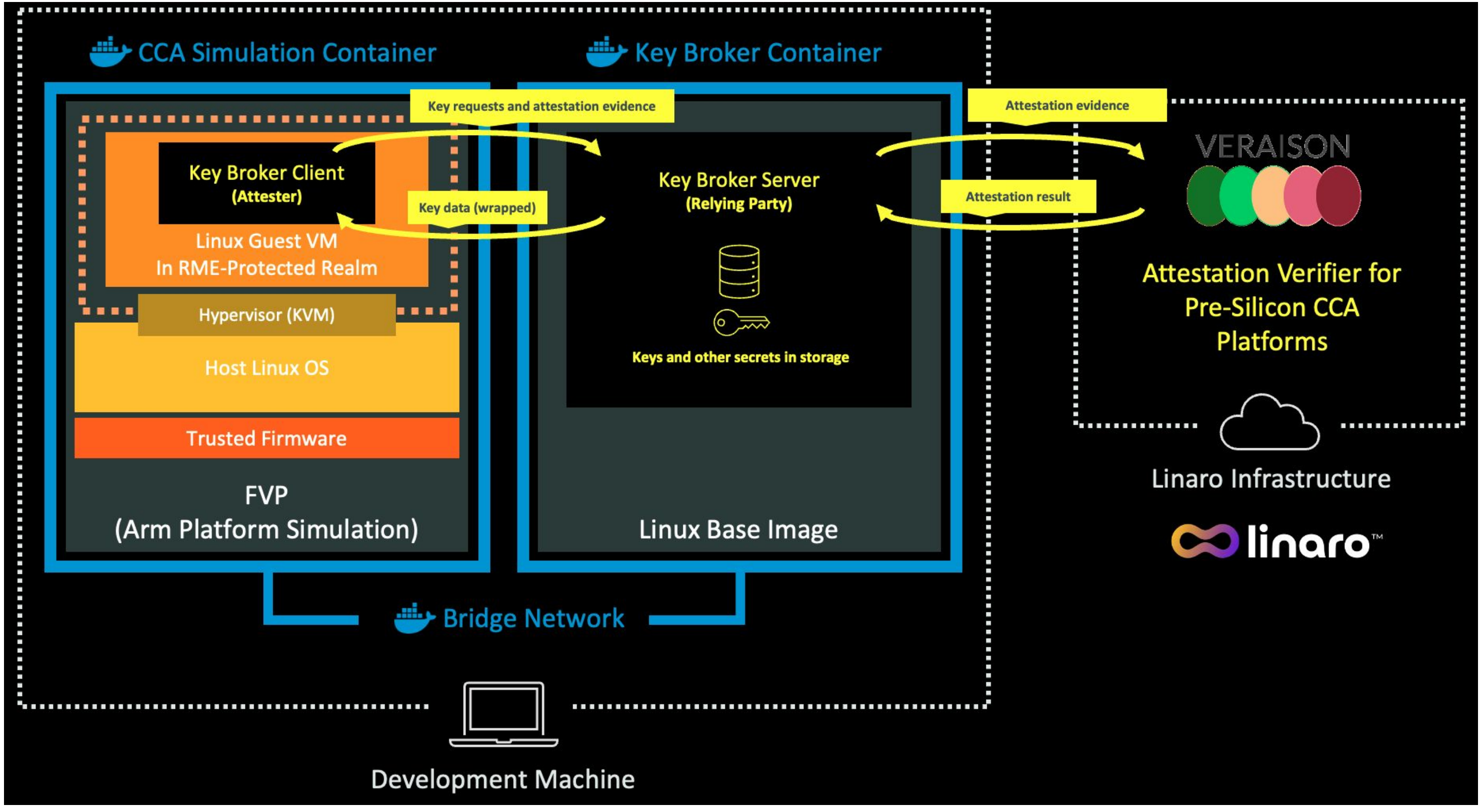




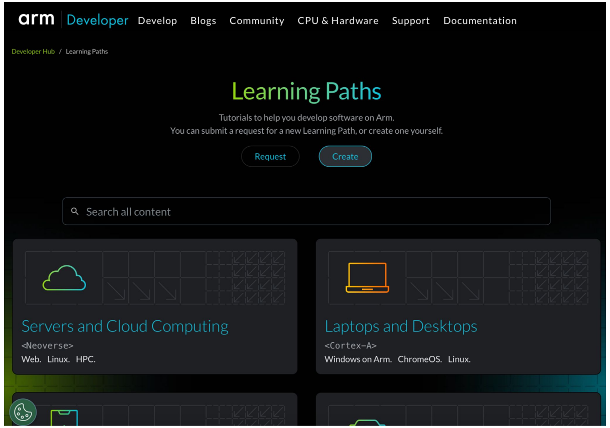
VERAISON

- Guided, end-to-end demonstrations
- Reusable open-source components, optimized for learning
- Uniform verifier back-end based on Veraison
- Convenient packaging and minimal dependencies
- No special hardware needed - supports software emulation
- Architecture neutral

Key Broker Example



Spreading the Word



arm Developer Develop Blogs Community CPU & Hardware Support Documentation
Developer Hub / Learning Paths

Learning Paths

Tutorials to help you develop software on Arm.
You can submit a request for a new Learning Path, or create one yourself.

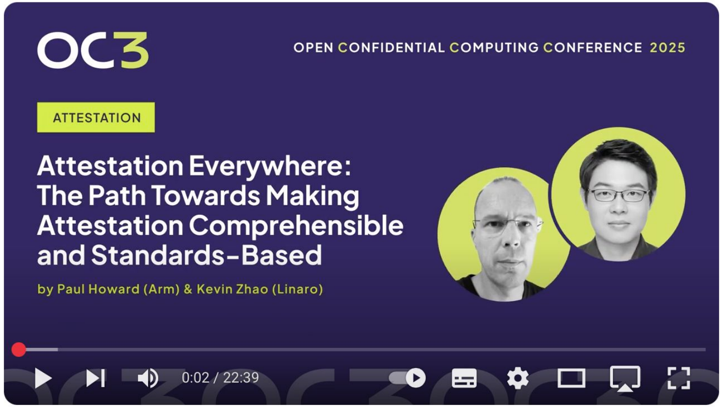
Request
Create
Search all content

Servers and Cloud Computing
<Neoverse>
Web. Linux. HPC.

Laptops and Desktops
<Cortex-A>
Windows on Arm. ChromeOS. Linux.

arm

https://learn.arm.com/



Attestation Everywhere: The Path Towards Making Attestation Comprehensible and Standards-Based

by Paul Howard (Arm) & Kevin Zhao (Linaro)

OC3

https://www.youtube.com/watch?v=c4lyaG-lTug

Onwards

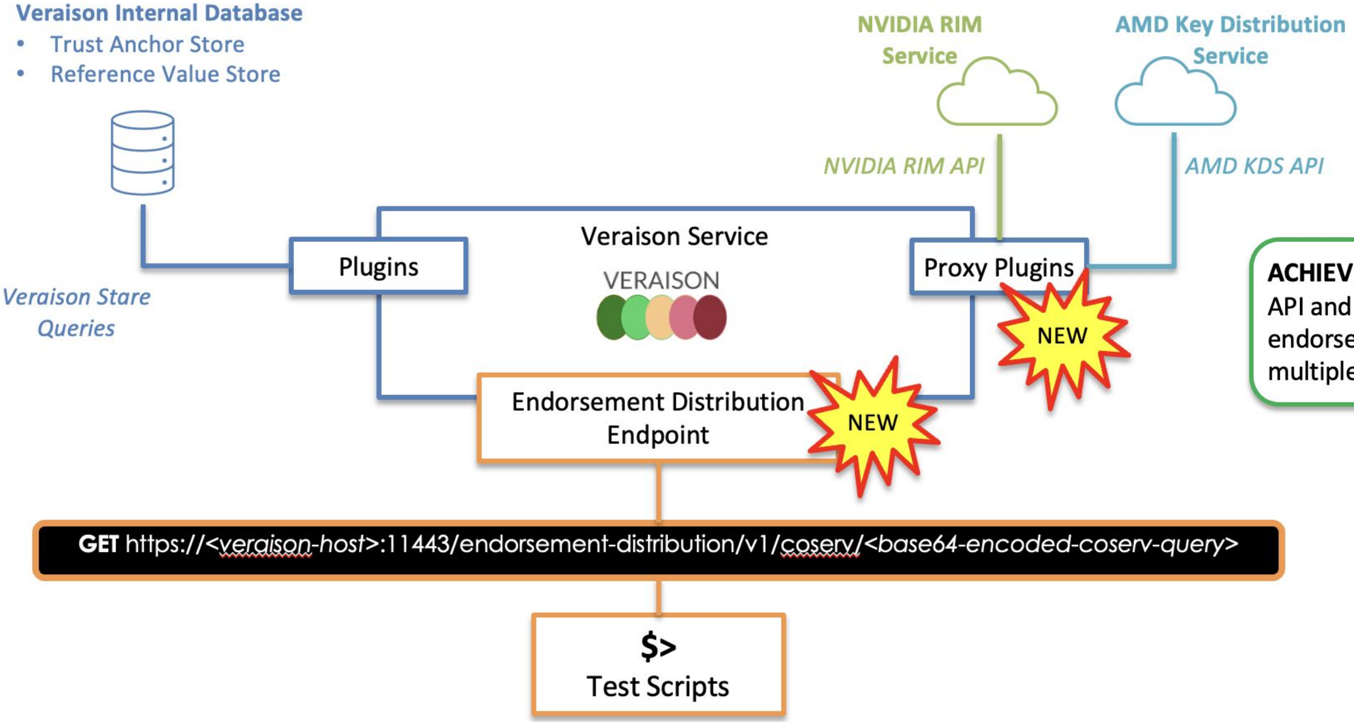
- More attestation patterns
  - Secure channel establishment (attested TLS)
  - Encrypted disk boot
  - Virtual TPMs
- Non-attestation concepts
- Contribute, contribute, contribute!!

CONFIDENTIAL COMPUTING CONSORTIUM

Bonus Content: Endorsement Distribution Standard (Proposed)

Objective: We evolved understanding of attestation and aligned on protocols and formats (e.g., **standardize the protocols in IETF RATS** and TLS WGs and coordinate with IRTF UFMRG for formal analysis)

IETF-123 Hackathon in Madrid - with Veraison!


Veraison Internal Database
- Trust Anchor Store
- Reference Value Store
Veraison Store Queries
Plugins
Veraison Service
VERAISON
Proxy Plugins
NEW
NVIDIA RIM Service
NVIDIA RIM API
AMD Key Distribution Service
AMD KDS API
Endorsement Distribution Endpoint
NEW
GET https://<veraison-host>:11443/endorsement-distribution/v1/coserv/<base64-encoded-coserv-query>
$>
Test Scripts

ACHIEVED: Demonstrated a **single**, common API and query language to distribute endorsements and reference values from multiple real-world supply chain sources ✓

Learn More

- CoSERV IETF draft: https://datatracker.ietf.org/doc/draft-howard-rats-coserv/
- Attestation SIG Presentation: https://youtu.be/MGRzP722EFg?si=UwXCuepVvmTnvrHs&t=942
- Veraison Dev Branch: https://github.com/veraison/services/tree/coserv

TAC discussion:

Research Fund Proposal for Academic projects

Confidential Computing Consortium Research Fund

Topic Schedule 2025

Date	Rotating Chair	CCC Project Topic	TAC Goal Topic
2025-09-18	~~AMD~~ Yash	Veraison	~~AMD~~ Arm
2025-10-02	Dan / Yash		AMD / Google

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

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

Thank You

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Maintenance

Glossary

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

Minutes

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

TAC 2025 Objectives

Update

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

TBD:

- Howard
- Henry / Kevin

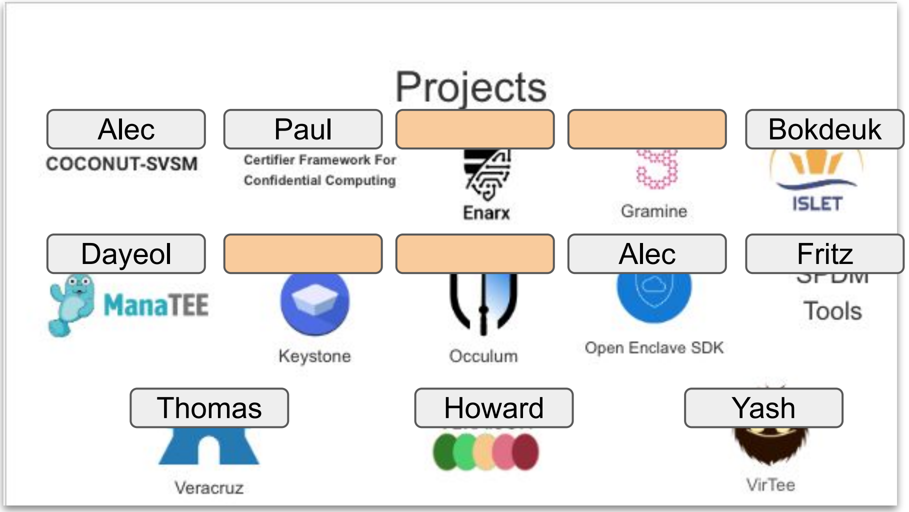
https://docs.google.com/document/d/1pa6XrOUhkIEFIP1MlLtn_84OjxV12L5hogch0shJkaA/edit?tab=t.0

Project Liaisons

Nathaniel

Henry

Bob



Projects

Alec
COCONUT-SVSM

Paul
Certifier Framework For Confidential Computing

Enarx

Gramine

Bokdeuk
ISLET

Dayeol
ManaTEE

Keystone

Occulum

Alec
Open Enclave SDK

Fritz
SPDM Tools

Thomas
Veracruz

Howard

Yash
VirTee

Dan
Attestation

Catherine
Kernel

Mark
GRC

Mark
TWI