Technical Advisory Council (TAC) Meeting

January 13, 2022

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. **TAC Tech Talk: Homomorphic Encryption:** Rosario Cammarota
3. Approval of minutes
4. Action item review
5. Updates from Outreach Committee
6. **Annual Project Review:** Keystone
7. Common Terminology
8. Any other business

Roll Call, and Introductions of New Attendees

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

Member	**Representative**	**Email**
Accenture	Giuseppe Giordano	giuseppe.giordano@accenture.com
Ant Group	Zongmin Gu	zongmin.gzm@antgroup.com
ARM	Thomas Fossati / Michael	thomas.fossati@arm.com
Facebook	Eric Northup / Shankaran	digitaleric@fb.com
Google	Iulia Ion	iuliaion@google.com
Huawei	Zhipeng (Howard) Huang	huangzhipeng@huawei.com
Intel	Dan Middleton / Simon	dan.middleton@intel.com
Microsoft	Dave Thaler(*)	dthaler@microsoft.com
Red Hat/IBM	Lily Sturmann / Dimitrios	lsturman@redhat.com

**TAC chair*

CONFIDENTIAL COMPUTING CONSORTIUM

2. TAC Tech Talk: Homomorphic Encryption

CONFIDENTIAL COMPUTING CONSORTIUM

3. Approval of TAC Minutes from November 18th telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/11-Nov/TAC%20Minutes%202021-18-11.pdf

RESOLVED:

That the minutes of the Nov. 18th 2021 meeting of the Technical Advisory Council meeting of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

CONFIDENTIAL COMPUTING CONSORTIUM

3b. Approval of TAC Minutes from December 16th telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/12-Dec/TAC%20Minutes%202021-16-12.pdf

RESOLVED:

That the minutes of the Dec. 16th 2021 meeting of the Technical Advisory Council meeting of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

CONFIDENTIAL COMPUTING CONSORTIUM

3. Action Item Review

1. [Mike, Eric, Stephen, Zongmin, Grant/Mike, Dan/Aeva] Recommend diversity and inclusion trainings to their projects and report back to the TAC on whether the maintainers or the contributors will be taking it and when the expected completion date is.
2. [VMT Subteam] Meet with Stephen to identify the process for establishing VMT.
3. [Dan] Provide contact for Rust Hypervisor firmware.
4. [Nathaniel] Identify a definition that Enarx can fit into on the Common Terminology document and define what is the smallest unit (such as a confidential computation).
5. [Steve] Define a term that is wider than only protecting data.
6. [ALL] Review, comment and/or correct text in Common Terminology Document [ON AGENDA]

Project	Proposed by	TAC Approved	Tech. Charter	IP Assigned	Board Presentation	Board Approved	Annual Review	Mentor	Webinar
Enarx	Red Hat	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	14 JAN 2021	Mike Bursell	JAN 2021, Q1 2022
OE SDK	Microsoft	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	12 NOV 2020	Dave Thaler	MAR 2021
SGX SDK for Linux	Intel	31 OCT 2019			31 OCT 2019			(Simon Johnson)	
TCF	Intel	28 MAY 2020							
Gramine	UNC Chapel Hill	2 APR 2020	Yes	Yes	01 DEC 2021	15 SEP 2021	4 NOV 2021	Eric V	3 FEB 2022
Keystone	UC Berkeley	23 JUL 2020	Yes	Yes	24 JUN 2021	MAR 2021	(13 JAN 2022?)	Stephen	JUN 2021
Occlum	Ant Financial	20 AUG 2020	Yes	Yes	10 SEP 2020	15 SEP 2021	2 DEC 2021	Zongmin	MAY 2021
Veracruz	Arm	3 SEP 2020	Yes	Yes	19 NOV 2020	14 APR 2021	18 NOV 2021	Thomas F.	APR 2021
CCC-Attestation	TAC	Yes	Yes	N/A	18 MAR 2021	18 MAR 2021		Dan & Aeva	Veraison – NOV 2021

5. Updates from Outreach Committee

6. Annual Project Review: Keystone

7. Establishing common terminology (issue #79)

Github Issue:

- https://github.com/confidential-computing/governance/issues/79

Doc in progress:

- https://docs.google.com/document/d/1xZ6IX0w0jaWDbLMFNAybTF3FpLnQ5TJ98nzIWbsbFnY/edit#

Anjuna glossary slides from last meeting:

- https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/11-Nov/AnjunaDefinitions.pdf

8. Any other business

Date	CCC Project Review	TAC Tech Talk
13 JAN 2022	Keystone annual review	Homomorphic Encryption – Rosario Cammarota
27 JAN 2022	Veraison new project submission	OP-TEE - Julian Hall
10 FEB 2022		Outreachy
24 FEB 2022		Henk

- Announcement: 2022 Google Summer of Code - Brian

List of suggested future topics

- TCG past work on CC – Henk Birkholz (invited, date TBD) – FEB 24
- Results of Outreachy program – Nick – FEB 10
- Rust Hypervisor firmware: https://github.com/cloud-hypervisor/rust-hypervisor-firmware - Dan to provide contact
- IETF Trusted Execution Environment Provisioning (TEEP) work – Dave
- Logging and error reporting in confidential computing – Mike B.
- Confidential computing from the perspective of the network – Penglin & Eric V.
- DARPA Data Protection in Open Environments (DPRIVE) – Dan contacted